ワイヤレスアダプタ/ワイヤレス VPN ルータ

UNIVERGE WA シリーズ

取扱説明書 第 5.1c 版

ご注意
ご使用の前にこのマニュアルをよくお読みの上で、正しくお使いください。
お読みになったあとは、いつでもご覧になれる場所に必ず保管してください。

はじめに

このたびはワイヤレスアダプタ/ワイヤレスVPNルータ UNIVERGE WAシリーズをお買い上げいただきまことにありがとうございます。

ご使用前に本マニュアルをよくお読みになり、正しくお使いください。

お読みになったあとは、いつでもご覧になれる場所に必ず保管してください。

本マニュアルでは、本製品の設置、設定、保守を行う上で、必要となることを記述しています。

なお、本マニュアルでは、パソコンおよびネットワークについて基本的な操作や設定ができる方を対象に説明しています。パソコンの操作や一般的なネットワークの設定については、お使いの製品のマニュアルや市販の書籍等をご覧ください。

ご注意

(1) 本マニュアルの内容の一部、または全部を無断転載、無断複写することは禁止されています。

(2) 本マニュアルの内容については、将来予告なしに変更することがあります。

(3) 本マニュアルの内容については、万全を期して作成いたしましたが、万一ご不審な点や誤り、記載もれなどお気づきのことがありましたら、ご連絡ください。

(4) 運用した結果については、(3)項にかかわらずいかなる責任も負いかねますので、あらかじめご了承ください。

本製品について

■情報処理製品等電波障害自主規制について

本製品は、クラスＢ情報技術装置です。本製品は、家庭環境で使用することを目的としていますが、本製品がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをしてください。

ＶＣＣＩ－Ｂ

■内蔵データ通信モジュール(内蔵モジュール)について

WA1511 には電波法に基づく工事設計認証を取得した無線設備が組み込まれています。

■医療機関等での使用

本製品は、医療機器、原子力設備や機器、航空宇宙機器、輸送設備や機器など、人命にかかわる設備や機器、および高度な信頼性を必要とする設備や機器としての使用またはこれらに組み込んでの使用は意図されておりません。

これら設備や機器、制御システムなどに本製品を使用され、当社製品の故障により、人身事故、火災事故、社会的な損害などが生じても、当社ではいかなる責任も負いかねます。

設備や機器、制御システムなどにおいては、冗長設計、火災延焼対策設計、誤動作防止設計など、安全設計に万全を期されるようご注意願います。

■輸出する際のご注意

本製品（ソフトウェアを含む）は日本国内仕様であり、外国の規格等には準拠しておりません。本製品は日本国外で使用された場合、当社は一切責任を負いかねます。また、当社は本製品に関し海外での保守サービス及び技術サポート等は行っておりません。本製品は、輸出貿易管理令別表第１－９(７)項に定める輸出規制品に該当致しますので、日本国外へ持ち出す際には日本国政府の輸出許可等必要な手続きをお取りください。許可手続き等にあたり特別な資料が必要な場合には、販売元にご相談ください。

■あらかじめご了承ください

本製品の故障、誤動作、不具合、あるいは停電などの外部要因によって、通信の機会を逸した為に生じた損害等の純粋経済損害につきましては、当社は一切その責任を負いかねますので、あらかじめご了承ください。また、本製品の使用方法や設定方法を誤って使用した結果発生した通話料金やプロバイダ接続料金等の損失について、当社ではいかなる責任も負いかねますので、あらかじめご了承ください。

■ソフトウェア使用許諾契約について

本製品を使用することによって、お客様が使用許諾契約書の条項に拘束されたことに同意したものとします。使用許諾契約書に同意されない場合は、日本電気株式会社および NEC プラットフォームズ株式会社はお客様に本製品のソフトウェアの使用または複製のいずれも許諾できません。なお、ソフトウェア使用許諾契約書は、本書の末尾に掲載しています。

■本製品の環境配慮について

・省エネルギーについて
　消費電力の低減を考慮しています。

・包装材について
　古紙配合のダンボールを使用しています。

■廃棄方法について

本製品を破棄するときは法律や地方自治体の条例に従って産業廃棄物として適正処理してください。なおNECは法律にもとづき、使用済み製品（情報通信機器）の回収／再資源化等を有償にて行っています。
詳細はこちらのページ http://jpn.nec.com/eco/ja/product/recycle/it/index.html（2014年7月現在）をご覧ください。

（使用済み製品はリサイクル可能な貴重な資源です。使用済み製品の回収にご協力ください。）

■商標、ライセンス、コピーライトについて

UNIVERGE®は、日本電気株式会社の登録商標です。

NEC、NECロゴは、日本およびその他の国における日本電気株式会社の商標および登録商標です。
そのほかの会社名ならびに商標名は各社の商標または登録商標です。なお、本文中では TM や®は明記していません。

マニュアルの表記について

押下するキーの表記について

- 本マニュアルでは、キーボードで押下する表記を以下のように記述しています。

  [Ctrl]、 [z] ：1つのキーを示す場合

  [Ctrl]+z ：2つのキーを同時に押す場合（[Ctrl]キーを押しながら[z]キーを押す場合など）

  user ：コマンドなど一連の文字を示す場合は文字列で示し、[ ]では囲っていません。

その他の表記について

- コンソール画面の内容は、以下のような画面イメージを四角で表記しています。

- 注意する内容は、注意で始まる文章で説明しています。

  注意

- 知っておくと便利な内容は、メモで始まる文章で説明しています。

  メモ

安全にお使い頂くために

製品を安全に正しくお使い頂き、お客様やほかの人々への危害や、財産への損害を未然に防止するために、守って頂きたい事項を示しています。

■安全マークについて

使用している表示と図記号の意味は次の通りです。内容をよく理解してから、マニュアルをお読みください。

⚠警告	人が死亡する、または重傷を負う可能性が想定される内容を示しています。
⚠注意	人が傷害を負う可能性が想定される内容、および物的損害が想定される内容を示しています。

禁止 『～をしてはいけない』と行為の「禁止」を示しています。	**ぬれ手禁止** 製品をぬれた手で扱う行為の禁止を示しています。
分解禁止 製品を分解する行為の禁止を示しています。	**指示** 必ず実行していただきたい行為の「指示」を示しています。
水ぬれ禁止 製品を水のかかる場所で使用したり、水にぬらすなどして使用する行為の禁止を示しています。	**ＡＣアダプタをＡＣコンセントから抜け** 電源プラグをＡＣコンセントから抜く行為に指示するものです。

■電源に関するご注意

⚠警告

	本製品添付のＡＣアダプタ及び電源コードは日本国内ＡＣ１００Ｖ（５０／６０Ｈｚ）の電源専用です。 他の電源で使用すると、火災、感電、故障の原因となります。		ＡＣアダプタ及び電源コードは必ず本製品に添付のものをお使いください。　また、本製品に添付のＡＣアダプタ及び電源コードは他の製品に使用しないでください。 火災、感電、故障の原因となります。
	本製品のＡＣアダプタ及び電源コードの接続は、テーブルタップ、分岐コンセント、分岐ソケットを使用したタコ足配線にしないでください。 ＡＣコンセントが過熱、劣化し、火災、感電の原因となります。		差込口が２つ以上ある壁のＡＣコンセントに他の電気製品のＡＣアダプタを差し込む場合は、合計の電流値がＡＣコンセントの最大値を超えないように注意してください。 火災、感電、故障の原因となります。
	電源コードを傷つけたり、破損したり、加工したり、無理に曲げたり、引っ張ったり、ねじったり、たばねたりしないでください。また、電源コードの上にものを載せないでください。コードの破損による、火災、感電の原因となります。		本製品の近くのＡＣコンセントを使用し、電源プラグは確実に差し込んでください。 ＡＣアダプタに金属などが触れると、火災、感電の原因となります。
	ぬれた手で電源プラグをＡＣコンセントに抜き差ししないでください。 感電の原因となることがあります。		ＡＣアダプタ及び電源コードを抜くときは、必ず電源プラグを持って抜いてください。 ＡＣアダプタや電源コードの破損により、火災、感電の原因となることがあります。

⚠注意

ぬれた手で本体に触れないでください。

感電の原因となることがあります。

本製品を移動させる場合は、本製品の電源プラグをＡＣコンセントから抜き、外部の接続線を外したことを確認のうえ、行ってください。

コードが傷つき、火災、感電の原因となることがあります。

機器、およびケーブルを接続する場合には、必ず電源プラグをＡＣコンセントから抜いてください。

電源プラグをＡＣコンセントに接続したまま、機器およびケーブルの接続を行うと、感電の原因となることがあります。

本製品をご使用にならないときは、安全のため必ず電源プラグをＡＣコンセントから抜いてください。

本製品は、アルミ電解コンデンサを使用しています。アルミ電解コンデンサは長時間通電せずに保管すると性能が低下します。長時間ご使用にならない場合でも、安定してご使用いただくために１年に２時間程度は、電源を通電してください。

■保管および使用環境に関する ご注意

⚠警告

本製品の上や近くに小さな金属類を置かないでください。

本製品の中に入ったりした場合、火災、感電の原因となります。

本製品の上や近くに植木鉢、コップ、化粧品、薬品など、液体の入った容器を置かないでください。

製品にこぼれたり、本製品の中に入ったりした場合、火災、感電の原因となります。

本製品をふろ場や加湿器のそばなど、湿度の高いところ（湿度９０％をこえる、または結露する場所）では設置および使用しないでください。

火災、感電、故障の原因となります。

本製品の使用中や使用直後に高温になる場合があり、やけどなどの恐れがありますので注意してください。

付属部品（USB メモリ、ネジ等の小さい部品）は幼児の手の届かない所に保管してください。万が一、飲み込んでしまった場合はすぐに医師の治療を受けてください。

⚠注意

本製品や電源コードを火気やストーブなどの熱器具に近づけないでください。

カバーや電源コードの破損により、火災、感電、故障の原因となることがあります。

本製品を直射日光の当たるところや、温度の高いところ（４５℃をこえる）に置かないでください。

本製品を油飛びや湯気があたるような場所、ほこりの多い場所に置かないでください。

火災、感電、故障の原因となることがあります。

温度変化の激しい場所（クーラーや暖房機のそばなど）に置かないでください。

本製品内部に結露が発生し、火災、感電、故障の原因となります。

⚠注意

本製品の通風孔をふさがないでください。 通風孔をふさぐと内部の温度が上がり、火災の原因となることがあります。	本製品の上に他の製品を重ねて置かないでください。 内部温度が上がり、火災の原因となることがあります。
本製品を不安定な場所（ぐらついた台の上や傾いた所など）に置かないでください。また、本製品の上に重い物を置かないでください。 落ちたりして、けがの原因となることがあります。	本製品を横置きで使用する場合は、ゴム足が下になるように置いてください。 倒れたり、落ちたりして、けがの原因となることがあります。
本製品を振動、衝撃の多い場所に置かないでください。 落ちたりして、けがの原因となることがあります。	本製品を縦置きで使用する場合は、添付のスタンドを使用して、両側は十分なスペースを確保してください。 倒れたり、落ちたりして、けがの原因となることがあります。
本製品は垂直面以外の壁や天井などには取り付けないでください。また、衝撃や振動を加えないでください。 振動などで落ちたりして、けがの原因となることがあります。	

本製品をラジオやテレビなどのすぐそばで使用するとラジオやテレビに雑音が入ることがあります。また、強い磁界を発生する製品が近くにあると、逆に本製品に雑音が入ってくることがあります。このような場合は離して使用してください。

本製品は、別途購入のデータ通信端末を使用します。利用するデータ通信端末の取扱説明書をご覧になり、本書とあわせて正しいお取り扱いをしてください。また、電波環境がよい場所に設置をしてください。電波の弱いところでは、接続出来ない等、状況により無線通信に影響が発生する可能性があります。

■禁止事項

<table>
<tr><td colspan="4">⚠警告</td></tr>
<tr><td></td><td>本製品内部の点検・調整・清掃・修理は、危険ですから絶対に行わないでください。
本製品内部の点検、調整、清掃、修理は、販売元にご連絡ください。</td><td></td><td>本製品内部の分解•改造は絶対に行わないでください。
火災、感電、故障の原因となります。</td></tr>
<tr><td></td><td>本製品の通風孔などの開口部から内部に、金属類や燃えやすいものなどの異物を入れないでください。
そのまま使用すると、火災、感電、故障の原因となることがあります。</td><td></td><td>本製品に水などの液体が入ったり、本製品をぬらしたりしないようにご注意ください。
火災、感電、故障の原因となります。</td></tr>
<tr><td colspan="4">⚠注意</td></tr>
<tr><td></td><td>本製品の上に物を載せたり、本製品に乗ったりしないでください。
壊れたりして、けがの原因となることがあります。</td><td></td><td>通信コネクタにケーブルを接続する前に必ず正しいケーブルであることを確認してください。
異なったケーブルを接続すると、火災、感電、故障の原因となることがあります。</td></tr>
</table>

■異常時およびトラブルに関するご注意

<table>
<tr><td colspan="2">⚠警告</td></tr>
<tr><td>万一、本製品を落としたり、破損したりした場合、電源プラグをＡＣコンセントから抜いて、販売元にご連絡ください。
そのまま使用すると、火災、感電、故障の原因となります。</td><td>電源コードが傷んだ（芯線の露出、断線など）場合、すぐに電源プラグをＡＣコンセントから抜いて、販売元にご連絡ください。
そのまま使用すると、火災、感電、故障の原因となります。</td></tr>
<tr><td>万一、本製品の内部に水などの液体が入った場合、電源プラグをＡＣコンセントから抜いて、販売元にご連絡ください。
そのまま使用すると、火災、感電、故障の原因となります。</td><td>万一、本製品から煙が出ている、変な臭いがするなどの異常状態のときは、すぐに電源プラグをＡＣコンセントから抜いて、煙が出なくなることを確認して、販売元にご連絡ください。
そのまま使用すると、火災、感電の原因となります。</td></tr>
<tr><td>万一、異物が本製品の内部に入った場合、電源プラグをＡＣコンセントから抜いて、販売元にご連絡ください。
そのまま使用すると、火災、感電、故障の原因となります。</td><td></td></tr>
<tr><td colspan="2">⚠注意</td></tr>
<tr><td>雷が鳴っているときは、ＡＣアダプタに触れたり、機器の接続をしたりしないでください。
雷によっては、感電の原因となることがあります。</td><td>落雷のおそれがあるときには、必ず電源プラグをＡＣコンセントから抜いてご使用をお控えください。
雷によっては、火災、感電の原因となることがあります。</td></tr>
</table>

■お手入れに関するご注意

⚠注意

水滴がついている場合は、乾いた布でふき取ってください。

本製品の電源プラグとACコンセントの間にほこりをためないようにときどき清掃してください。また、電源プラグがしっかりと差し込まれているかときどき確認してください。

火災の原因となることがあります。

内部にほこりがたまったまま長い間掃除をしないと、火災、故障の原因となることがあります。１年に１度は内部の掃除を販売元にご相談ください。

本製品のお手入れを行う際には、安全のため必ず電源プラグをＡＣコンセントから抜いてください。

本製品の汚れは、やわらかい布に水、または中性洗剤を含ませて軽くふいてください。この時、安全のため必ずＡＣアダプタをＡＣコンセントから抜いてください。

ベンジン、シンナーなど（揮発性のもの）や薬品を用いてふいたりしますと、変形や変色の原因となることがあります。また、殺虫剤などをかけた場合も変形や変色の原因となることがありますのでご注意ください。

■無線（3G、LTE）使用に関するご注意

⚠警告

高精度な電子機器の近くでは本製品を使用しないでください。電子機器に影響を与える場合があります。
特に医療機器をお使いの場合は機器メーカーまたは販売店に電波の影響について確認ください。

弊社で指定しているアンテナ以外は使用しないでください。

植込み型医療機器などの近くで本製品を使用する場合は、電波によりそれらの機器に影響を与える可能性がありますので以下の点にご注意ください。

１.植込み型医療機器の使用者が15cm以内に近づく可能性のある場所に本体や無線アンテナを設置しないようにしてください。

2.医療機関の屋内で使用する場合は付近に医療機器が無い場所に設置してください。またその医療機関の機器管理者の指示に従ってください。

■USBメモリ使用に関するご注意

⚠警告

USBポートに接続したUSBメモリ内のファイルへアクセス中に、USBメモリを本製品から外したり、本製品の電源を切ったりすると、アクセス中のデータが壊れる可能性がありますので、ご注意ください。

梱包内容の確認

■各製品に添付されている小冊子をご参照ください。

「**UNIVERGE WA1020** お使いになる前に」

「**UNIVERGE WA1510/WA1511** お使いになる前に」

「**UNIVERGE WA2020** お使いになる前に」

「**UNIVERGE WA2021** お使いになる前に」

1

UNIVERGE WA シリーズの特長と機能

製品の主な特長

■ワイヤレスアダプタ　UNIVERGE WA1020

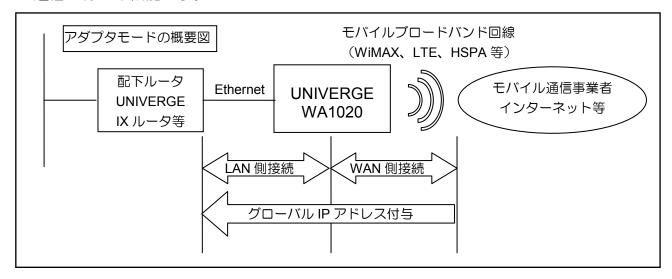
UNIVERGE WA1020（以下、WA1020と称す）は、モバイルブロードバンド網に接続するデータ通信端末を用いて、モバイル回線による通信事業者ネットワークへのアクセス用途に用いられるワイヤレスアダプタです。

WA1020には、「ルータモード」と「アダプタモード」の2つのモードがあります。WAN側インタフェースにHSPA等のデータ通信端末を接続することによりモバイル回線接続を実現します。

ルータモードとは・・・

WA1020のルータ機能として、IPsec機能、EtherIP機能、L2TPv3機能、ネットワークモニタ機能等があります。また、VLAN機能で複数セグメントの収容ができます。これらの機能を利用して、WA1020単体でモバイル回線を利用した、インターネットVPNによるネットワーク構築が可能になります。

アダプタモードとは・・・

配下に接続するルータがWA1020のWAN側に付与されるIPアドレスを用いて透過的な通信が行える機能です。

UNIVERGE WA1020 の利用シーン

- ワイヤレスアダプタとして動作することで、既存ルータの機能をフル活用し、モバイル回線の利用が可能です。
- WA1020と配下のルータを離れた場所に設置することで、モバイル通信の弱点である電波受信感度の問題を解消します。
- 単体でもワイヤレスVPNルータとして利用でき、イベント会場や工事現場の様な一時的に設置して利用される環境でも、WAN側回線工事が不要なのですぐに利用可能です。
- さまざまな設置環境に応えられるよう、横置き／縦置き／壁掛けに対応しています。

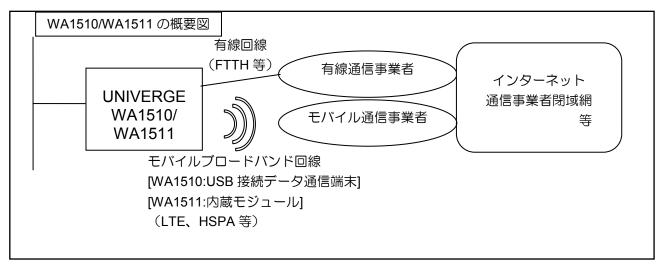
■ワイヤレスVPNルータ　UNIVERGE WA1510/WA1511

UNIVERGE WA1510、UNIVERGE WA1511（以下、WA1510、WA1511と称す）は、1台で有線回線とモバイル回線に接続することが可能な、ワイヤレスVPNルータです。

WA1510はWAN側インタフェースとして、FTTH等の高速な有線回線サービスに接続するためのGigabitEthernetポートを有しており、最大1Gbpsの高速な回線サービスに利用することができます。

加えて、LTEなどの高速のモバイルブロードバンドサービスに接続する、データ通信端末を利用することもできます。

WA1511はWAN側インタフェースとして、GigabitEthernetポートに加えて、LTEなどの高速のモバイルブロードバンドサービスに接続するデータ通信端末をモジュールとして内蔵しており、外付けアンテナ利用して、より安定した環境でのモバイル接続を可能となります。

ルータ機能としては、IPsec機能、EtherIP機能、L2TPv3機能、ネットワークモニタ機能等があります。これらの機能を利用して、WA1511単体でメイン回線として有線回線を利用し、バックアップ回線としてモバイル回線を利用した、インターネットVPNによる冗長構成のネットワーク構築が可能になります。

UNIVERGE WA1510/WA1511 の利用シーン

- 高速転送機能を有しているため、数百Mbps～1Gbpsの高速回線に接続する、インターネットアクセスルータとして利用できます。
- 有線回線をメイン回線とし、内蔵モジュールによるモバイル回線をバックアップ回線としたインターネットVPN用のVPNルータとして利用できます。
- 複数セグメントをタグVLANで収容し、インターネットアクセス兼ローカルルータとしても利用できます。

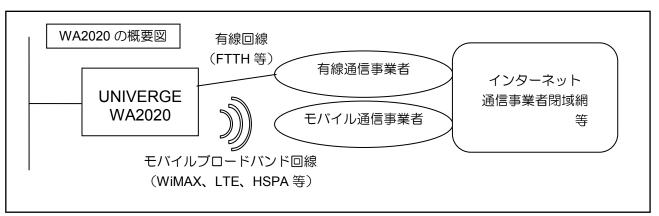
■ワイヤレスVPNルータ　UNIVERGE WA2020

UNIVERGE WA2020（以下、WA2020と称す）は、1台で有線回線とモバイル回線に接続することが可能な、ワイヤレスVPNルータです。

WA2020はWAN側インタフェースとして、FTTH等の高速な有線回線サービスに接続するためのGigabitEthernetポートを有しており、最大1Gbpsの高速な回線サービスに利用することができます。

加えて、LTEやWiMAXなどの高速のモバイルブロードバンドサービスに接続する、データ通信端末を利用することもできます。

また、LAN側インタフェースとして4ポートスイッチングHUB（全ポートGigabitEthernet）を有しており、パソコン等の複数の端末を接続することが可能です。
このスイッチングHUB（SW-HUB）ポートでVLAN機能を使用し、複数セグメントを収容することができます。

ルータ機能としては、IPsec機能、EtherIP機能、L2TPv3機能、ネットワークモニタ機能等があります。これらの機能を利用して、WA2020単体でメイン回線として有線回線を利用し、バックアップ回線としてモバイル回線を利用した、インターネットVPNによる冗長構成のネットワーク構築が可能になります。

UNIVERGE WA2020 の利用シーン

- 高速転送機能を有しているため、数百Mbps～1Gbpsの高速回線に接続する、インターネットアクセスルータとして利用できます。
- 有線回線をメイン回線とし、モバイル回線をバックアップ回線としたインターネットVPN用のVPNルータとして利用できます。
- 複数セグメントをVLANで収容し、インターネットアクセス兼ローカルルータとしても利用できます。

■ワイヤレスVPNルータ　UNIVERGE WA2021

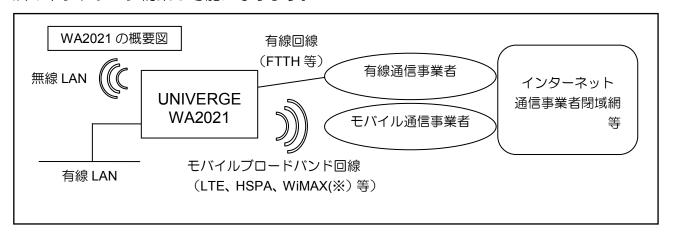
UNIVERGE WA2021（以下、WA2021と称す）は、1台で有線回線とモバイル回線に接続することが可能で、さらに無線LANアクセスポイントとして無線LAN子機を接続することが可能な、ワイヤレスVPNルータです。

WA2021はWAN側インタフェースとして、FTTH等の高速な有線回線サービスに接続するためのGigabitEthernetポートを有しており、最大1Gbpsの高速な回線サービスに利用することができます。

加えて、LTEやWiMAX(※)などの高速のモバイルブロードバンドサービスに接続する、データ通信端末を利用することもできます。

LAN側インタフェースとして4ポートスイッチングHUB（全ポートGigabitEthernet）を有しており、パソコン等の複数の端末を接続することが可能です。このスイッチングHUB（SW-HUB）ポートでVLAN機能を使用し、複数セグメントを収容することができます。

また、PCカードスロットにオプション品の無線LANカード「WA100-AP」を接続することで、無線LANアクセスポイントとして動作しますので、複数の無線LAN端末を接続することが可能です。

ルータ機能としては、IPsec機能、EtherIP機能、L2TPv3機能、ネットワークモニタ機能等があります。これらの機能を利用して、WA2021単体でメイン回線として有線回線を利用し、バックアップ回線としてモバイル回線を利用した、インターネットVPNによる冗長構成のネットワーク構築が可能になります。

<u>UNIVERGE WA2021 の利用シーン</u>

- 高速転送機能を有しているため、数百Mbps～1Gbpsの高速回線に接続する、インターネットアクセスルータとして利用できます。
- 有線回線をメイン回線とし、モバイル回線をバックアップ回線としたインターネットVPN用のVPNルータとして利用できます。
- 複数セグメントをVLANや無線LANで収容し、インターネットアクセス兼ローカルルータとしても利用できます。

（※）WiMAXと無線LANアクセスポイントは同時に使用できません。

IPsec機能概要

IPsecとは、IP security Protocol の略でIPパケットを暗号化し、安全に通信を行うためのプロトコルでInternet-VPNに利用されています。

主な特長として、暗号化、認証の機能があります。暗号化としては、データの暗号化により機密性の確保が可能です。認証としては、通信相手の認証とパケットの改ざん検出が可能です。

IPsecは、以下の機能をサポートしています。

暗号化

ESP（Encapsulated Security Payload）を使用したIPパケット全体の暗号化を行うトンネルモード、IPパケットのデータ部分のみ暗号化を行うトランスポートモード

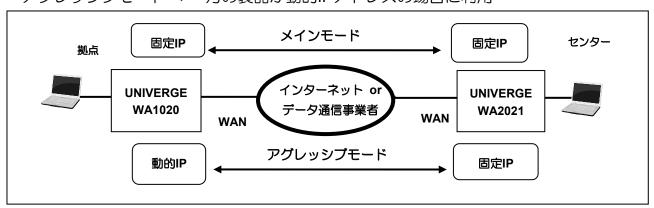
本製品で利用可能なアルゴリズム

	利用可能なアルゴリズム
暗号化プロトコル （共通鍵認証）	DES（default）、3DES、 AES-128、AES-192、AES-256、 Null
認証プロトコル （メッセージ認証）	MD5（default）、SHA1 、SHA2
Diffie-Hellman グループ （DH グループ）	DH group 1（768）、DH group 2（1024） DH group 5（1536）、DH group 14（2048） ※PFS（Perfect Forward Secrecy）も上記と同じ DH グループで利用できます。

鍵交換タイプ

メインモードとアグレッシブモードをサポートしています。接続する回線種別（IPアドレスの割当方法）によって、鍵交換タイプの選択が可能です。

メインモード　　　　：IPsecの両端の製品が固定IPアドレスを有している場合に利用

アグレッシブモード　：一方の製品が動的IPアドレスの場合に利用

IPsec拡張機能

- NATトラバーサル

  IPsecで暗号化されたパケット（ESPパケット）をNAPT変換できるようにする機能です。IPsecの対向装置までの経路上にNAPT機器が存在する場合に利用します。

- IPsecトンネル内のNAT/NAPT変換

  IPsecにて暗号化するパケットに対して、暗号化前にNAT/NAPT変換を行う機能です。

- PeerFQDN機能

  動的IPアドレス対向の環境において、ダイナミックDNSと組み合わせることで、対向装置のIPアドレスをFQDN指定することが可能となり、IPsec接続を確立することが可能です。

IPsec接続性向上

- IPsec SA削除要求送信機能

  IPsec SAが不一致の状態でIPsecパケットを受信した場合に、IPsec SA削除要求を出すことで、IPsec通信を復旧（再確立）させる機能です。

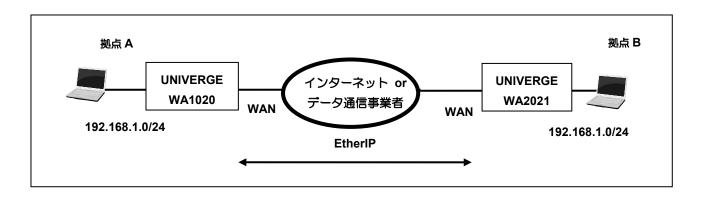
- INITIAL-CONTACT送信機能

  IPsec通信中に、装置の再起動等によりSAを消失した場合、対向装置からのIPsecパケットを受信した際に、INITIAL-CONTACTを送信することで、IPsec通信を復旧（再確立）させる機能です。

EtherIP機能概要

EtherIPとは、イーサネットフレームをIPパケットでカプセル化し、離れた拠点間をブリッジ接続する機能です。イーサネットフレームのカプセル化方式として、EtherIPを使用しています。

* EtherIP: Tunneling Ethernet Frames in IP Datagrams

また、IPsec機能と組み合わせて利用することで、インターネット網を利用したL2VPNを実現することが可能です。本製品のEtherIPの対地数は、1対地となります。

<u>**EtherIP関連機能**</u>

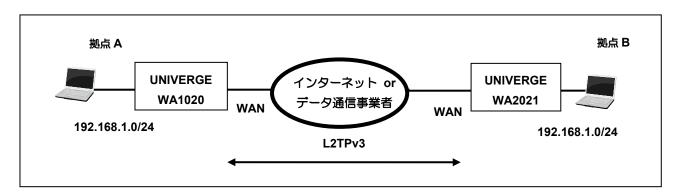
- MACフィルタ機能を有しているため、受信したイーサネットフレームの種別を指定した廃棄が可能です。
- EtherIPの対象となるデータに対して、TCP MSS(MaxSegmentSize)の自動調整が可能です。

L2TPv3 機能概要

L2TPv3とは、イーサネットフレームをIPパケットでカプセル化し、離れた拠点間をブリッジ接続する機能です。イーサネットフレームのカプセル化方式として、L2TP version 3（RFC3931準拠）を使用しています。

* L2TPv3: Layer Two Tunneling Protocol - Version 3 (L2TPv3)

また、IPsec機能と組み合わせて利用することで、インターネット網を利用したL2VPNを実現することが可能です。本製品のL2TPv3の対地数は、2対地となります。

L2TPv3は、EhterIPをサポートしていない対向装置（主にCisco製ルータ）とのL2VPN構築に適しています。

L2TPv3関連機能

- MACフィルタ機能を有しているため、受信したイーサネットフレームの種別を指定した廃棄が可能です。
- L2TPv3の対象となるデータに対して、TCP MSS(MaxSegmentSize)の自動調整（固定値）が可能です。
- ブリッジプロテクト機能を有しているため、2方路以上のインタフェースがブリッジに参加する場合、ループ構成を防ぐことが可能です。

L2TPv3とEhterIPの主な差分点

- L2TPv3はコネクション型で、EtherIPはコネクションレス型です。
- L2TPv3セッション確立時に対向装置の認証ができます。
- L2TPv3はHelloを利用したセッションの維持、死活監視ができます。
- L2TPv3の対地数は2対地です。
- ネットワークモニタ機能を利用して、L2TPv3セッションの冗長構成が可能です。

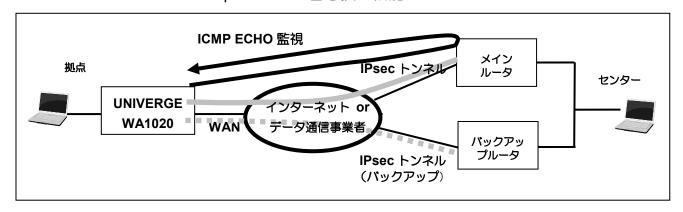
ネットワークモニタ機能概要

ネットワークモニタ機能は、定期的にICMP ECHOを送信し、接続先への到達性を監視することでネットワーク障害の発生、復旧を検出し、迂回ルートへの切り替えや製品の再起動を行い、通信の復旧や、異常状態からの復旧をすることができます。

ネットワークモニタ機能では、主に以下の監視設定を行うことができます。

- ICMP ECHOの送信間隔
- 障害発生、復旧までのICMP ECHOの失敗、成功回数
- ICMP ECHOのウェイトタイム
- 監視有効化または、製品の起動から監視開始までのディレイ時間
- ICMP ECHOの送信インタフェース、ネクストホップアドレス、ソースアドレス
- 監視するインタフェースの種類、復旧レイヤ

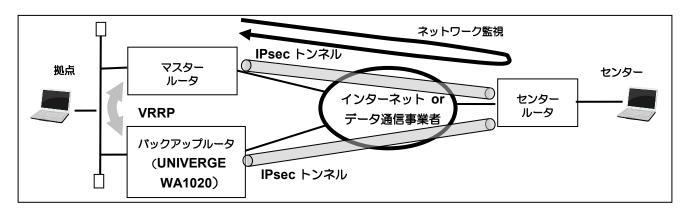
発生、復旧を検出した場合に実行できる主な処理は以下のとおりです。

- スタティックルートの削除／追加
- 製品の再起動
- バックアップランプ（BAK）の点灯（WA1510、WA1511、WA2020、WA2021）
- 他モニタグループ監視の開始／停止
- Proxy DNSサーバアドレスの追加／削除
- IPsec SA／IKE SAの削除
- VRRPシャットダウン機能によるVRRP起動/停止
- L2TPv3シャットダウン機能によるL2TPv3起動/停止
- インタフェースシャットダウン機能によるモバイル回線の切断/接続
- L2TPv3インタフェースのpeer/source書き換え機能

VRRP機能概要

VRRP機能は、１つのグループに所属した複数のルータのうち１つのルータを通常の通信に使用し、そのルータに障害が発生した際に別のルータにバックアップさせることで、LAN側を冗長させる機能です。

VRRP機能を用いて、以下のような利用ができます。

ルータバックアップ

VRRP機能を有する一組のルータを、同じLAN上で同じVRRPグループとすることで、一方のルータ（マスタルータ）が故障した場合に、他方のルータ（バックアップルータ）をその故障したルータのバックアップとして動作させ、LAN側の端末に対してデフォルトゲートウェイを冗長することができます。

本製品では、以下のような機能があります。

- ネットワークモニタ連携
- 複数VRRPグループ
- 仮想IPに対するIPホスト機能（ping、telnet等）

VLAN機能概要

VLAN機能により、１つの物理的なインタフェースを仮想的に複数のセグメントに分割して利用することが可能となります。

本製品では、以下のように VLAN 機能を搭載しています。

VLAN種別	WA1020	WA1510 WA1511	WA2020 WA2021
タグVLAN	○(FE0ポート)	○(GE0ポート、GE1ポート)	○(GE0ポート、GE1ポート)
ポートVLAN	－	－	○(GE1ポート)

○：サポート　　－：未サポート

なお、VLAN機能を利用する場合の注意点や、VLAN機能と併用できないルータ機能については、本取扱説明書の＜付録＞をご参照ください。

タグVLAN機能

タグVLAN機能では、ベースとなる物理インタフェースに、タグVLAN ID（VID）を指定したVLANインタフェースを複数割り当てることで、VLANフレームを送受信することができます。

このタグVLAN機能を使用することで、1つのインタフェースを仮想的に複数のセグメントとして利用することができます。

- 装置として、最大16個のVLANインタフェース(VLAN0からVLAN15)が設定できます。
- VLANインタフェースは、タグVLAN ID（VID）が一致するVLANフレームのみ、送受信を行います。
- ベースインタフェースでは非VLANフレームのみ、VLANインタフェースではVLANフレームのみ送受信動作を行います。（ハイブリッド動作）
- WA2020、WA2021のGigaEthernet1.0では、VLANインタフェースにSW-HUBポートを関連付けることで、他のSW-HUBポートとブロードキャストドメインを分割することができます。（ポート指定動作）

ポートVLAN機能

ポートVLAN機能では、WA2020、WA2021のGE1のLAN1～LAN4の各スイッチポートに対して、それぞれ１つのVLANインタフェースを割り当てることができます。

このポートVLAN機能を使用することで、LAN1～LAN4の各スイッチポートを独立したセグメントとして使用する事ができ、複数のルータポートとして使用することができます。

Web-GUI機能概要

本製品は、Web-GUI機能をサポートしており、コマンドラインインタフェースに用いる設定コマンドを使用することなく、WWWブラウザから装置の設定及び操作を行うことができます。

Web-GUI機能は特別な設定をすることなく、初期状態にてご使用になれます。

またWeb-GUIへのアクセスは、SSLプロトコルを使用しており安全性が高められております。

本製品を初期状態でご使用になる場合、WWWブラウザでログインする際には以下のように設定します。

URLアドレス：https://192.168.1.200/

ユーザ名　　：admin

パスワード　：admin

Web-GUIでは、以下のような設定が可能です。

- 基本設定
- 有線回線
- モバイル回線
- 無線LAN (WA2021のみ)
- IPsec設定
- ルーティング
- アクセスリスト
- その他

また、装置の状態監視や保守のためのメンテナンス機能として、以下の機能もあります。

<u>状態監視</u>

・装置状態…装置基本情報、インタフェース状態、モバイル回線状態、VPN状態、DDNS状態

・ログ表示

<u>保守</u>

・保存、再起動

・バージョンアップ

・通信試験

Web-GUIのご利用方法については、Web-GUIマニュアルをご参照ください。

Dynamic DNS機能概要

本製品は、Dynamic DNSに対応する機能を搭載しています。

本機能を使用することで、LTEやHSPA、WiMAX等のサービスにおける動的IPアドレス環境下からドメイン名（FQDN）を使用して、WAシリーズや配下機器にアクセスすることが可能となります。

■WAシリーズ専用Dynamic DNSサービス

本製品はNECプラットフォームズ株式会社が提供するWAシリーズ専用Dynamic DNSサービスを利用することができ、このサービスは以下の特徴があります。

サービス料金　：　無料

申込み／登録　：　不要

※サービス自体を利用するための申込み／登録は不要ですがサービスの運用状況などをお知らせするメーリングリストに参加いただくための利用者情報の登録をお願いします。

設定方法　：　WAシリーズ本体で設定

WAシリーズ専用Dynamic DNSサービスのご利用に際しては、以下の注意事項をよく読んでご利用ください。

- ベストエフォート型のサービスとなります。接続保証するものではありません。
- 設備メンテナンス等により予告なくサービスを停止する場合があります。また、サービス提供者の都合により、サービスを終了する可能性があります。
- Dynamic DNSサーバに登録される FQDN は装置固有のものとなり、任意の FQDN を登録することはできません。

また、WAシリーズ専用Dynamic DNSサービスの他に、他の事業者が提供するDynamic DNSサービスのご利用が可能です。他の事業者が提供するDynamic DNSサービスのご利用にあたっては各サービスにおける利用許諾や条件等をご確認頂き、同意の上でご利用願います。
事業者毎の設定方法につきましてはコマンドリファレンスマニュアルをご参照ください。

尚、本機能は、他の事業者が提供するDynamic DNSサービスにおける動作を保証するものではありません。サービス側の仕様変更などにより、ご利用できない場合があります。

無線LAN機能概要

WA2021は無線LAN機能をサポートしております。
（WA1020、WA1510、WA1511、WA2020は非サポート）

本機能と別売の無線カード(WA100-AP)と組み合わせることで、WA2021を無線LANアクセスポイントとして利用することが可能となります。

本製品では、以下のような無線LANアクセスポイント機能を搭載しています。

機能名	対応内容
マルチSSID	最大４つ
動作モード	IEEE802.11b/g/n 2.4GHz帯(2400～2484MHz) 、1～13ch(固定)/1～11ch(自動選択)
伝送方式	IEEE802.11b: DS-SS（スペクトラム直接拡散）方式 IEEE802.11g: OFDM（直交周波数分割多重）方式 ／ 搬送波数 52 IEEE802.11n: OFDM（直交周波数分割多重）方式 搬送波数 [HT20]56[HT40]114、MIMO（空間多重）方式
伝送速度	IEEE802.11b:11/5.5/2/1Mbps IEEE802.11g: 54/48/36/24/18/12/9/6Mbps IEEE802.11n: [HT20]130/117/104/78/52/39/26/19.5/13Mbps [HT40]300/270/243/216/162/108/81/54/40.5/27/13.5Mbps (自動フォールバック)
セキュリティ	WEP(152/128/64bit) WPA-PSK(TKIP/AES)、WPA2-PSK(TKIP/AES)

無線LAN機能

無線LAN機能を用いることで、複数の無線LAN子機を収容することができます。

- 装置として、最大4個のSSID(WirelessEthernet0.0からWirelessEthernet0.3)が設定できます。

ひとつのSSIDをひとつのネットワークインタフェースとして扱うことが可能です。

その他の機能

■モバイル回線 IP 着信機能

NTTドコモ社「ビジネスmoperaアクセスプレミアム」FOMAタイプによるN2502データ通信端末使用において、ルータモード動作にて、IP着信機能（パケット着信）に対応しています。（但し、WA1510、WA1511、WA2021は非対応）

なお、本機能使用時において、同時にLAN側への発呼とmopera側からの着呼が発生した場合、発呼と着呼の両方が共に停止する場合があります。

最大1分ほどで復旧しますので、IP着信機能使用時はご留意ねがいます。

■運用／管理／監視機能

- SNMP機能、SYSLOG機能を使用することで本製品の管理／監視が可能です。また、ローカルコンソール、リモートコンソール（telnet、SSH）からのCLI（コマンドラインインタフェース）による設定が可能です。
- 自動更新機能を使用することで、指定した日時に自動的にソフトウェアのバージョンアップを行うことが可能です。
- HSPA用のPPPにおいて、切断スケジュール機能をサポートしています。
  通信業者の仕様によっては、連続回線接続をしていると一定時間ごとに網から回線切断が行われる場合があります。あらかじめ切断時間をスケジュールする事で、業務時間中やバッチ処理等の通信処理中に回線切断が発生しないように、定期的な回線切断のタイミングを避けることができます。

■メール送信機能

メール送信機能により、Syslogや、データ通信端末で取得したIPアドレス等の通知が可能です。管理者に送付する事で日々の管理の利便性が向上します。

メール送信機能で送信できる情報は以下になります。

- Syslog送信機能

  本製品のメモリ上に記録されているSyslogを1日に1回メールで送信する事ができます。これにより、直接、本製品に接続してSyslogを確認することなく情報を確認する事ができます。

- IPアドレス通知機能

  WAN側インタフェース等において、回線が接続した際に取得するIPアドレスを送信することができます。これにより、本製品が動的に取得するIPアドレスを管理者が把握することが可能となり、ダイナミックDNSを利用することなく、リモートからの接続が可能になります。

■**SSH サーバ機能**

Secure SHell(セキュアシェル)を使用し、暗号や認証により、telnetより安全にリモートコンソール接続が可能となります。（SSHv2のみ対応）

■**USB ストレージ機能**

オプションのUSBメモリを使用することで、以下の機能が利用できます。

- フラッシュメモリ内のプログラムファイルやコンフィグレーションファイルのバックアップ。
- syslogのバックアップ。
- 障害時等の情報収集を行うテクニカルサポート情報の保存。
- 運用に使用するプログラムファイル、スタートアップコンフィグを保存したUSBメモリ接続による、運用設定への自動更新。

USBストレージ機能が使用できるUSBメモリは、オプション品として購入できます。
オプション品以外の市販のUSBメモリは使用することはできません。

■**ポリシールーティング機能**

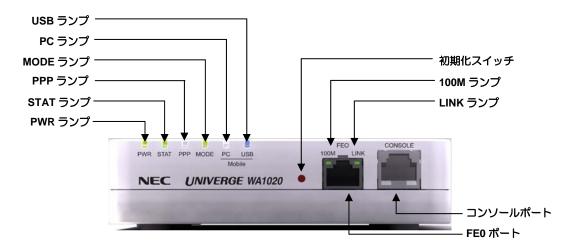
通常のスタティックルートだけではなく、ルートマップ、アクセスリストを使用したポリシーに基づいたルーティングが使用できます。ルートマップやアクセスリストを組みあわせて、より詳細なルート設定が指定できます。ソースアドレスによるルーティング、出力インタフェース指定、ネクストホップ指定、インタフェースの受信適用指定等の設定ができます。また、自発の通信に関してもポリシーによるルート設定の指定ができます。

2

各部の名称とはたらき

各部の名称

■WA１０２０

・ 前面（表示ランプ）

前面ポート一覧

名　称	機能説明
初期化スイッチ	本製品を工場出荷状態に戻すスイッチです。（電源オン時） またアンテナレベルを取得する際にも使用します。（運用中）(注 1)
FE0 ポート	本製品を LAN に接続するためのポートです。
コンソールポート	本製品の設定を行う際に PC 等のコンソール端末を接続するポートです。

注1） 初期化スイッチを押したまま、電源を起動することで、設定を工場出荷状態に戻します。工場出荷状態に戻す詳細方法については、「6章 管理と保守」の「初期化スイッチを使用する方法」項目をご参照ください。

運用中に初期化スイッチを短押し（2秒以上）で離すと、データ通信端末のアンテナレベルをリアルタイムで取得し、LEDランプで表示します。（電波サーベイモード）装置を設置する際に、適切な電波受信感度を確保できるようご利用ください。

電波サーベイモード

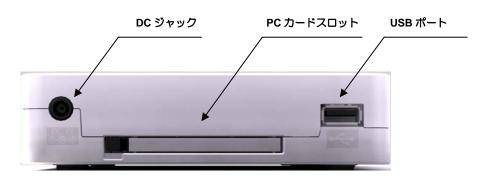
Serial0インタフェースを使用した接続では、一部のデータ通信端末を除き、PPP接続中はアンテナレベルを取得する事ができません。PPP接続中に初期化スイッチを短押しすると、PPPを一時的に切断し、1分間の電波サーベイモードとなり、アンテナレベルを取得します。アンテナレベルは、STAT LEDランプおよびコンソールで確認することができます。電波サーベイモード終了後は、PPPを再接続し、元の状態に戻ります。

- “show mobile status”コマンドでデータ通信端末のアンテナレベル取得状態を確認できます。アンテナ取得状態中は“antenna status”項目が“Standby”と表示されます。また、電波サーベイモード中は、“Survey”と表示されます。
- MobileEthernetインタフェースを利用した接続では、回線接続中でもアンテナレベルが取得可能です。
- 電波サーベイ機能はソフトウェアバージョン4.0.0から対応しています。

LED ランプ表示一覧

表　示		ランプ状態	機能説明
PWR		消灯	電源が OFF 状態
		緑点灯	電源が ON 状態
		緑点滅	USB メモリのファームウェア／スタートアップコンフィグ自動更新起動中
STAT		消灯	ブートモニタが起動中
		赤点灯	自己診断中状態
		赤点滅	フラッシュメモリまたは、USB メモリアクセス中
		緑点灯	運用状態
		緑点滅	電波サーベイモード
PPP		消灯	PPP セッションが確立していない状態
		緑点灯	PPP セッションが確立中
		緑点滅（早い）	ダイヤルアップ中
		緑点滅（遅い）	PPP ネゴシエーション中
		橙点灯	IPsec 接続中 または L2TPv3 接続中
		赤点灯	ユーザ認証失敗
		赤点滅	ダイヤルアップエラー
MODE		消灯	ルータモード状態
		緑点灯	アダプタモード状態
Mobile	PC	消灯	PC カードが接続されていない状態
		赤点滅	データ通信端末が異常な状態、または基地局からの電波状態が異常な状態 (注 1)
		赤点灯	圏外（基地局からの電波が受信できない状態） (注 1)
		青点滅（早い）	電波受信感度：可
		青点滅（遅い）	電波受信感度：良
		青点灯	電波受信感度：優
	USB	消灯	USB が接続されていない状態
		赤点滅	データ通信端末が異常な状態、または基地局からの電波状態が異常な状態 (注 1)
		赤点灯	圏外（基地局からの電波が受信できない状態） (注 1)
		青点滅（早い）	電波受信感度：可
		青点滅（遅い）	電波受信感度：良
		青点灯	電波受信感度：優
		紫点灯	未接続検出機能または給電 OFF 機能により、USB への給電を OFF した状態
FE0	100M	消灯	10Mbps でリンク確立またはしていない状態
		緑点灯	100Mbps でリンク確立している状態
	LINK	消灯	イーサネットのリンクが確立していない状態
		緑点灯	イーサネットのリンクが確立中
		緑点滅	データの送受信が行われている状態

注1） アンテナレベル0 リカバリ機能を設定した際は、圏外を検出すると赤点滅になります。アンテナレベル0 リカバリ機能は、コマンドマニュアルをご参照ください。

・ 背面（コネクタ、スイッチ）

背面操作箇所一覧

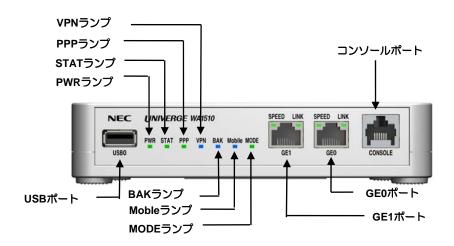
名　称	機能説明
DC ジャック	AC アダプタ電源を接続するジャックです。
PC カードスロット	PC カードタイプのデータ通信端末を接続するためのスロットです。(注 1、3)
USB ポート	USB タイプのデータ通信端末または USB メモリを接続するポートです。(注 1、2)

注1）　サポートしていないデータ通信端末は、スロット／ポートに差し込まないでください。

注2）　USBハブ経由やUSB延長ケーブルを使用しないでください。

注3）　データ通信端末の活線挿抜はサポートしておりませんので、電源OFFの状態でデータ通信端末の挿抜を行なってください。

■WA１５１０／WA１５１１

・ 前面（表示ランプ）

※WA1511 は、「WA1510」表記が「WA1511」となる以外は、同じ構成です。

前面ポート一覧

名　称	機能説明
GE1 ポート(LAN)	本製品を LAN に接続するためのポートです。
GE0 ポート(WAN)	本製品を WAN に接続するためのポートです。
コンソールポート	コンソール端末を接続するポートです。
USB ポート(USB0)	USB タイプのデータ通信端末または USB メモリを接続するためのポートです。　(注 1、2、3、4)

注1）　サポートしていないデータ通信端末や USB メモリは、USB ポートに差し込まないでください。

注2）　USB ハブ経由や USB 延長ケーブルを使用しないでください。

注3）　WA1511 では USB タイプのデータ通信端末をサポートしていませんので、接続しないでください。USB メモリのみのサポートとなります。

注4）　WA1510、WA1511 は、WiMAX データ通信端末をサポートしておりません。

LED ランプ一覧

表　示		ランプ状態	機能説明
PWR		消灯	電源が OFF 状態
		緑点灯	電源が ON 状態
		緑点滅	USB メモリのファームウェア／スタートアップコンフィグ自動更新起動中
STAT		消灯	ブートモニタが起動中
		赤点滅	フラッシュメモリまたは、USB メモリアクセス中
		赤点灯	自己診断エラー(注 1)
		緑点灯	運用状態
		緑点滅	電波サーベイモード(注 3)
PPP(注 2)		消灯	PPP セッションが確立していない状態
		橙点灯	ユーザ認証失敗
		橙点滅	ダイヤルアップエラー
		緑点滅(早い)	ダイヤルアップ中
		緑点滅(遅い)	PPP ネゴシエーション中
		緑点灯	PPP セッションが確立中
VPN		消灯	IPsec 未接続
		青点灯	IPsec 接続中または L2TPv3 接続中
BAK（注 6）		消灯	下記以外の状態
		青点灯	無線バックアップ動作中
Mobile（注 4）		消灯	データ通信端末/内蔵モジュールが動作していない状態
		赤点滅	データ通信端末/内蔵モジュールが異常な状態、または基地局からの電波状態が異常な状態 (注 5)
		赤点灯	圏外（基地局からの電波が受信できない状態） (注 5)
		青点滅(早い)	電波受信感度：可
		青点滅(遅い)	電波受信感度：良
		青点灯	電波受信感度：優
		紫点灯	未接続検出機能または給電 OFF 機能により、USB ポート及び内蔵モジュールへの給電を OFF にした状態(注 7)
MODE		橙点灯	給電 OFF 機能により、WA1511 の USB0 ポートへの給電を OFF にした状態
		—	将来拡張用
GE0/GE1	SPEED	消灯	10Mbps でリンク確立またはリンクが確立していない状態
		橙点灯	100Mbps でリンク確立している状態
		緑点灯	1Gbps でリンク確立している状態
	LINK	消灯	イーサネットのリンクが確立していない状態
		緑点灯	イーサネットのリンクが確立中
		緑点滅	データの送受信が行われている状態

注 1）起動時には自己診断が行われ、この間は PWR、STAT、PPP、VPN、BAK、Mobile、MODE のランプが点灯します。

注 2）複数の PPP セッションを利用する場合、各回線の状態が PPP ランプで表示されます。ただし、状態が変化した PPP セッションの状態を優先して表示されます。

注 3）電波サーベイモードは WA1510 で、対応する USB タイプデータ通信端末接続時で表示されます。

注 4）WA1510 の場合、データ通信端末利用時以外は、消灯しています。

注 5）アンテナレベル 0 リカバリ機能を設定した際は、圏外を検出すると赤点滅になります。

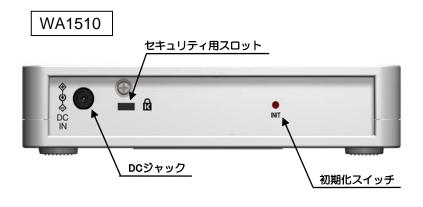
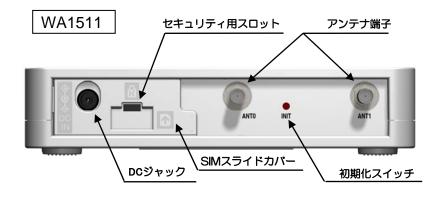
注 6）BAK ランプはネットワークモニタ機能を制御することで点灯させることが出来ます。

注 7）WA1511 の内蔵モジュールは、装置内部で USB 接続されており、給電 OFF コマンドで制御します。

・ 背面（コネクタ、スイッチ）

WA1510

WA1511

背面操作箇所一覧

名　称	機能説明
DC ジャック(DC IN)	AC アダプタ電源を接続するジャックです。（注 1）
SIM スライドカバー	SIM カードを取り替える場合に右にスライドさせます。 ※WA1511 のみ
セキュリティ用スロット	盗難防止用鍵取付スロットです。市販のセキュリティワイヤを取り付けることで、本製品を盗難から守ります。（注 2）
初期化スイッチ(INIT)	本製品を工場出荷状態に戻すスイッチです。（電源投入時） （注 3）
アンテナ用端子	内蔵モジュール用のアンテナの接続端子です。ANT0、ANT1 の 2 端子です。（注 4） ※WA1511 のみ

注 1）添付の AC アダプタ以外は接続しないでください。

注 2）セキュリティ用スロットに取り付ける市販のセキュリティワイヤは、T 型ロックのカギの形状によっては穴に入らない場合があります。セキュリティワイヤは、形状に注意して準備してください。

注 3）初期化スイッチを押したまま電源を起動すると、工場出荷状態に戻ります。
工場出荷状態に戻す詳細方法については、「6 章 管理と保守」の「初期化スイッチを使用する方法」項目をご参照ください。

WA1510 では、運用中に初期化スイッチを短押し（2 秒以上）で離すと、データ通信端末のアンテナレベルをリアルタイムで取得し、LED ランプで表示します。（電波サーベイモード）
装置を設置する際に、適切な電波受信感度を確保できるようご利用ください。

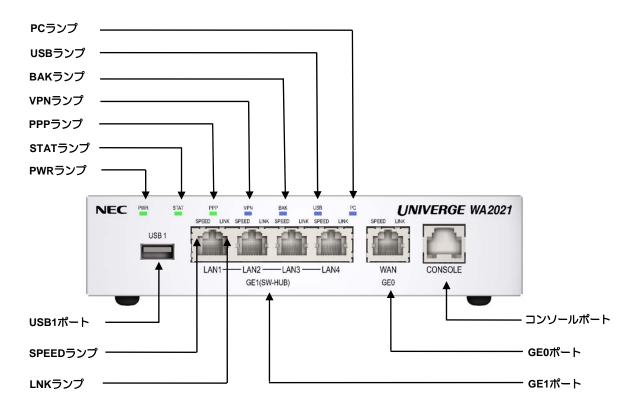
注 4）同梱のアンテナもしくは専用オプションアンテナ以外は使用しないでください。
アンテナは 2 本一組です。必ず 2 本とも接続するようにしてください。

電波サーベイモード

Serial0インタフェースを使用した接続では、一部のデータ通信端末を除き、PPP接続中はアンテナレベルを取得する事ができません。PPP接続中に初期化スイッチを短押しすると、PPPを一時的に切断し、1分間の電波サーベイモードとなり、アンテナレベルを取得します。アンテナレベルは、STAT LEDランプおよびコンソールで確認することができます。電波サーベイモード終了後は、PPPを再接続し、元の状態に戻ります。

- “show mobile status”コマンドでデータ通信端末のアンテナレベル取得状態を確認できます。アンテナ取得状態中は“antenna status”項目が“Standby”と表示されます。また、電波サーベイモード中は、“Survey”と表示されます。
- MobileEthernetインタフェースを利用した接続では、回線接続中でもアンテナレベルが取得可能です。
- 電波サーベイ機能はソフトウェアバージョン4.0.0から対応しています。

■WA2020／WA2021

・ 前面（表示ランプ）

前面ポート一覧

名　称	機能説明
GE1 ポート(LAN1-4)	本製品を LAN に接続するためのポート(SW-HUB)です。
GE0 ポート(WAN)	本製品を WAN に接続するためのポートです。
コンソールポート	コンソール端末を接続するポートです。
USB ポート(USB1)	USB タイプのデータ通信端末または USB メモリを接続するポートです。(注 1、2、3)

注1）　サポートしていないデータ通信端末、無線LANカードは、スロット／ポートに差し込まないでください。

注2）　USBハブ経由やUSB延長ケーブルを使用しないでください。

注3）　データ通信端末、無線LANカード（WA2021のみ）の活線挿抜はサポートしておりませんので、電源OFFの状態でデータ通信端末の挿抜を行なってください。

LED ランプ表示一覧

表　示		ランプ状態	機能説明
PWR		消灯	電源が OFF 状態
		緑点灯	電源が ON 状態
		緑点滅	USB メモリのファームウェア／スタートアップコンフィグ自動更新起動中
STAT		消灯	ブートモニタが起動中
		赤点滅	フラッシュメモリまたは、USB メモリアクセス中
		赤点灯	自己診断エラー(注 1)
		緑点灯	運用状態
		緑点滅	電波サーベイモード
PPP(注 4)		消灯	PPP セッションが確立していない状態
		橙点灯	ユーザ認証失敗
		橙点滅	ダイヤルアップエラー
		緑点滅(早い)	ダイヤルアップ中
		緑点滅(遅い)	PPP ネゴシエーション中
		緑点灯	PPP セッションが確立中
VPN		消灯	IPsec 未接続
		青点灯	IPsec 接続中 または L2TPv3 接続中
BAK(注 5)		消灯	下記以外の状態
		青点灯	無線バックアップ動作中
USB(注 3)		消灯	USB が接続されていない状態
		赤点滅	データ通信端末が異常な状態、または基地局からの電波状態が異常な状態 (注 2)
		赤点灯	圏外（基地局からの電波が受信できない状態） (注 2)
		青点滅(早い)	電波受信感度：可
		青点滅(遅い)	電波受信感度：良
		青点灯	電波受信感度：優
		紫点灯	未接続検出機能または給電 OFF 機能により USB0 への給電を OFF した状態
PC (注 3)	データ通信端末使用時	消灯	PC カードが接続されていない状態
		赤点滅	データ通信端末が異常な状態、または基地局からの電波状態が異常な状態 (注 2)
		赤点灯	圏外（基地局からの電波が受信できない状態） (注 2)
		青点滅(早い)	電波受信感度：可
		青点滅(遅い)	電波受信感度：良
		青点灯	電波受信感度：優
		紫点灯	未接続検出機能または給電 OFF 機能により USB1 への給電を OFF した状態、(PC カードタイプのデータ通信端末使用時は紫点灯しません)
	無線 LAN カード使用時 (WA2021)	消灯	PC カードが接続されていない状態
		青点滅(100ms)	通信中
		青点滅(500ms)	子機帰属可能状態 (アクセスポイントとして動作している状態)
		青点灯	電波を送信していない状態 (WirelessEthernet0.x が全て shutdown 状態)
GE0/ GE1	SPEED	消灯	10Mbps でリンク確立またはリンクが確立していない状態
		橙点灯	100Mbps でリンク確立している状態
		緑点灯	1Gbps でリンク確立している状態
	LINK	消灯	イーサネットのリンクが確立していない状態
		緑点灯	イーサネットのリンクが確立中
		緑点滅	データの送受信が行われている状態

注1） 起動時には自己診断が行われ、この間はPWR、STAT、PPP、VPN、BAK、USB、PCのランプが点灯します。

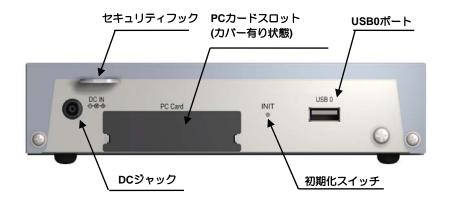
注2） アンテナレベル0 リカバリ機能を設定した際は、圏外を検出すると赤点滅になります。アンテナレベル0 リカバリ機能は、コマンドマニュアルをご参照ください。

注3） 2つのUSBポート(USB0/USB1）にそれぞれWiMAXデータ通信端末とWiMAX以外のデータ通信端末を実装して使用する場合は、USBランプはWiMAXデータ通信端末の状態を示し、PCランプは接続しているUSBポート番号に関わらずWiMAX以外のデータ通信端末の状態を表示します。
PCカードタイプのデータ通信端末を実装して使用する場合は、PCランプは、PCカードタイプのデータ通信端末の状態を優先して表示します。
USB0の給電をOFFにして、USB1でデータ通信端末を実装して使用する場合は、USBランプはUSB0の給電OFF表示が優先され、USB1のデータ通信端末の状態は、表示されません。

注4） 複数のPPPセッションを利用している場合は、状態が変化したPPPセッションの状態を優先して表示します。全てのPPPセッションが確立している場合は緑点灯、全てのPPPセッションが確立してない場合は消灯します。

注5） BAKランプはネットワークモニタ機能を制御することで点灯させることが出来ます。

・ 背面(コネクタ、スイッチ)

背面操作箇所一覧

名　称	機能説明
DC ジャック(DC IN)	AC アダプタ電源を接続するジャックです。
PC カードスロット (PC Card)	PC カードタイプのデータ通信端末を接続するためのスロットです。使用する際は、カバー（マグネット）を外してからご利用ください。(注 1、3、4)
セキュリティフック	盗難防止用の鍵取付穴です。市販のセキュリティワイヤを取り付けることで、本製品を盗難から守ります。(注 5)
初期化スイッチ(INIT)	本製品を工場出荷状態に戻すスイッチです。（電源オン時） またアンテナレベルを取得する際にも使用します。（運用中）(注 6)
USB ポート(USB0)	USB タイプのデータ通信端末または、USB メモリを接続するためのポートです。(注 1、2、3)

注1）　サポートしていないデータ通信端末、無線LANカード（WA2021のみ）は、スロット／ポートに差し込まないでください。

注2）　USBハブ経由やUSB延長ケーブルを使用しないでください。

注3）　データ通信端末、無線LANカード（WA2021のみ）の活線挿抜はサポートしておりませんので、電源OFFの状態でデータ通信端末の挿抜を行なってください。

注4）　PCカードタイプのデータ通信端末、無線LANカード（WA2021のみ）をご使用にならない場合は、PCカードスロットにカバーを付けた状態でご利用ください。カバーはPCカードスロットから製品内に入り込まないように注意願います。もしカバーが製品内に入ってしまった場合は、PCカードスロットから取り除いてください。

注5）　セキュリティフックに取り付ける市販のセキュリティワイヤは、カギの形状によってはフックに入らない場合があります。セキュリティワイヤは、形状に注意して準備してください。

注6）　初期化スイッチを押したまま、電源を起動することで、設定を工場出荷状態に戻します。工場出荷状態に戻す詳細方法については、「6章 管理と保守」の「初期化スイッチを使用する方法」項目をご参照ください。

運用中に初期化スイッチを短押し（2秒以上）で離すと、データ通信端末のアンテナレベルをリアルタイムで取得し、LEDランプで表示します。（電波サーベイモード）装置を設置する際に、適切な電波受信感度を確保できるようご利用ください。

電波サーベイモード

Serial0インタフェースを使用した接続では、一部のデータ通信端末を除き、PPP接続中はアンテナレベルを取得する事ができません。PPP接続中に初期化スイッチを短押しすると、PPPを一時的に切断し、1分間の電波サーベイモードとなり、アンテナレベルを取得します。アンテナレベルは、STAT LEDランプおよびコンソールで確認することができます。電波サーベイモード終了後は、PPPを再接続し、元の状態に戻ります。

- “show mobile status”コマンドでデータ通信端末のアンテナレベル取得状態を確認できます。アンテナ取得状態中は“antenna status”項目が“Standby”と表示されます。また、電波サーベイモード中は、“Survey”と表示されます。
- MobileEthernetインタフェースを利用した接続では、回線接続中でもアンテナレベルが取得可能です。
- 電波サーベイ機能はソフトウェアバージョン4.0.0から対応しています。

周辺機器との接続

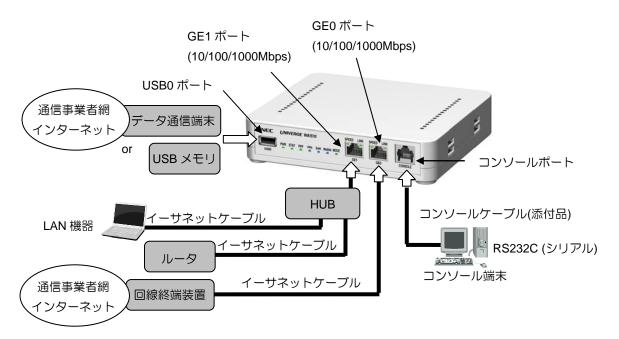
■ネットワーク接続形態について

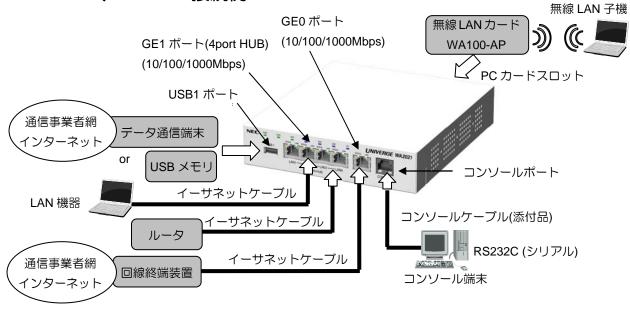
本製品は、さまざまなネットワークを接続することができます。

- **WA1020接続例**

USB メモリ
or
データ通信端末
通信事業者網
インターネット
FE0 ポート
(10/100Mbps)
USB ポート
PC カードスロット
コンソールポート
イーサネットケーブル
LAN 機器
HUB
コンソールケーブル(添付品)
イーサネットケーブル
RS232C (シリアル)
ルータ
コンソール端末

注意 WA1020のFE0ポートを通信事業者が提供するWAN環境、回線終端装置に接続しないで下さい。

- **WA1510、WA1511接続例**

注意 WA1511のUSB0ポートは、データ通信端末の接続はサポートしていません。

- **WA2020、WA2021接続例**

注意　無線LAN機能はWA2021のみサポートしています。

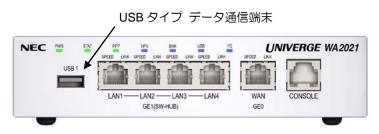
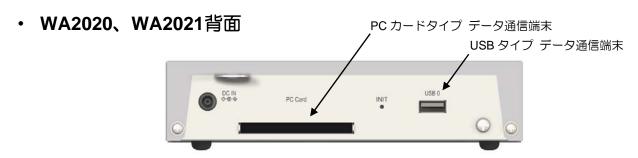
■データ通信端末の接続について

データ通信端末を利用してモバイル回線に接続する場合は、データ通信端末のコネクタ形状に合わせて、装置の PC カードスロットもしくは USB ポートにデータ通信端末を接続します。

- **WA1020背面**

- **WA1510正面**

- **WA2020、WA2021正面**

- **WA2020、WA2021背面**

利用できるデータ通信端末は以下をご参照ください。
http://jpn.nec.com/univerge/wa/

注意 PCカードやUSBは、上記参照先の機器以外動作を保証しておりません。他のPCカードやUSB機器（無線通信以外の機器を含む）を接続して、不具合や故障等が発生した為に生じた損害等については責任を負いかねますので、あらかじめご了承ねがいます。

注意　PCカードやUSBにデータ通信端末を接続し、認識できないなどの問題が発生した場合、本体からすみやかに外すようにしてください。

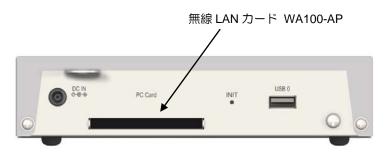
注意　USBハブ経由やUSB延長ケーブルでは接続しないでください。

注意　データ通信端末(PCカード)の活線挿抜はサポートしておりませんので、電源OFFの状態でデータ通信端末の挿抜を行なってください。

注意　データ通信端末を接続してご利用になる場合には、データ通信端末にて指定されている環境条件範囲内でのご利用を推奨致します。

■無線 LAN カードの接続について

無線 LAN アクセスポイント機能を使用する場合は、装置の PC カードスロットにオプション品の無線 LAN カード「WA100-AP」を接続します。

- **WA2021背面**

注意　無線LAN機能は、WA2021とWA100-APの組合せでのみ動作します。他の無線LANカードを接続して、不具合や故障等が発生した為に生じた損害等については責任を負いかねますので、あらかじめご了承ねがいます。

注意　無線LANカード接続は、無線LANカードの取扱説明書を参照してください。

注意　無線LANカード WA100-APの活線挿抜はサポートしておりませんので、電源OFFの状態で挿抜を行なってください。

■イーサネットケーブルの接続について

FE0、GE0、GE1 ポートは、Auto-MDI/MDIX 動作のため、ストレート結線またはクロス結線を意識する事なく接続できます。ケーブルは、UTP または STP ケーブルを使用してください。

ルータ、PC など、本製品と接続する製品に応じてご用意ください。

また、通信モードは初期設定が通信速度、通信方式とも Auto ですので、接続する機器も Auto であれば自動で最適なモードに設定します。ただし、接続する機器が固定設定の場合は、通信モードを固定設定する必要があります。

以下は、各ポートの対応する設定一覧です。

通信モード、メディアタイプ		通信モード						メディアタイプ		
設定	Interface	Auto	10M half	10M full	100M half	100M full	1G full	Auto	MDI	MDIX
WA1020	FE0	○	○	○	○	○	―	○	×	×
WA1510/ WA1511	GE0	○	○	○	○	○	○	○	×	×
	GE1	○	○	○	○	○	○	○	×	×
WA2020/ WA2021	GE0	○	○	○	○	○	○	○	○	○
	GE1	○	○	○	○	○	○	○	○	○

注意　FE0ポートに接続する対向製品との通信を100BASE-TXで行う場合には、カテゴリ5以上のUTPまたはSTPケーブルをご使用ください。

注意　GE0、GE1ポートに接続する対向製品との通信を1000BASE-Tで行う場合には、カテゴリ5e以上のUTPまたはSTPケーブルをご使用ください。

注意　通信モードがautoでも、GE0、GE1ポートのモードと接続する対向製品のモードが合わない場合があります。その際は、接続する対向製品との通信モードを固定設定で合わせてご使用ください。

■コンソールポートの接続について

コンソールポートには、本製品の基本的な設定を行うためのローカルコンソール（PC 等）を接続します。

接続するケーブルは、本製品添付のコンソールケーブルをご使用ください。ローカルコンソール側が 25 ピン端子の場合には、市販の D-SUB25 ピン変換コネクタを使用してください。

ローカルコンソールとして使用する PC またはワークステーション等の端末には、VT-100 準拠の通信ソフトウェアが必要です。

注意　ローカルコンソールから、本製品の設定を変更する等以外で、特に使用することがないときは必ずコンソールポートからコンソールケーブルを抜いてください。

注意　通信ソフトは次の設定にします。

項目	設定
通信速度	9600bps
データ長	8bit
パリティ	なし
ストップビット	1bit
フロー制御	なし

■AC アダプタの接続について

DC プラグを本体に接続してから AC アダプタの電源プラグを AC100V（50Hz/60Hz）の AC コンセントに接続します。

注意　付属のACアダプタ以外は使用しないでください。
　　　また、付属のACアダプタは他の製品に使用しないでください。

注意　本製品の近傍にACコンセントを用意し、かつACアダプタが、容易にACコンセントから抜き差しできるように空間を空けるようにしてください。

3

設置と準備

設置場所

■設置場所について

本製品は、前後左右5cm、上5cm以内に他の製品や壁などが無い場所に設置してください。ただし壁掛けの場合は、壁掛け面を除きます。

本製品を縦置きで使用する場合は、添付のスタンドを使用してください。

また、動作不良や故障、感電等の原因となることがあるので、次のような場所へは設置しないでください。

●不安定（ぐらついた台の上や傾いた所）な場所

●直射日光のあたる場所

●水または薬品のかかるおそれのある場所

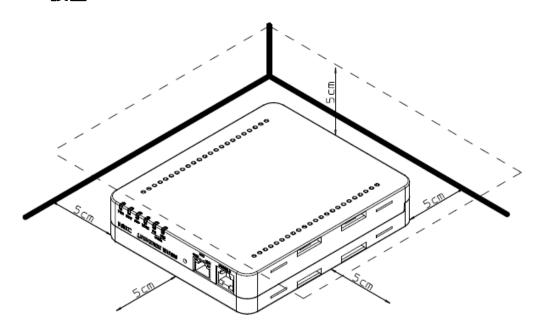
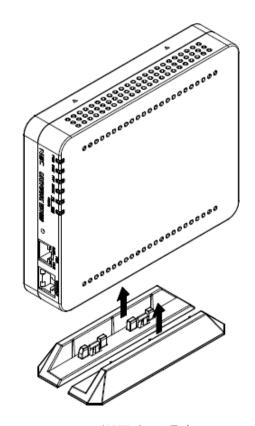
●製品の上に重量物を載せた設置

●ほこりの多い場所

●放熱を妨げる所、通気性の悪い場所

●強い磁気を発生する機器が近くにある場所

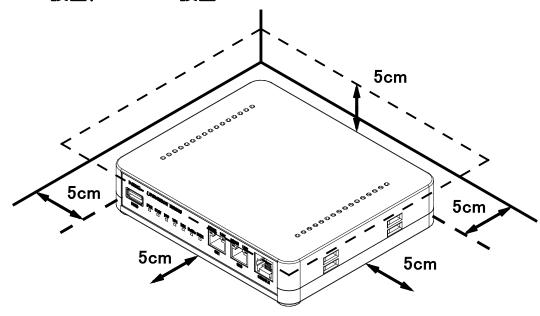
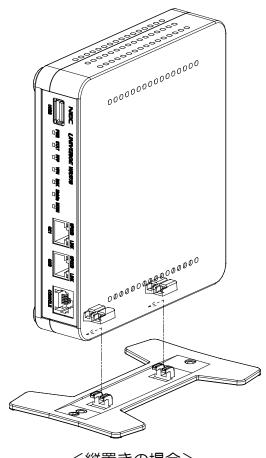
●発熱する機器の上

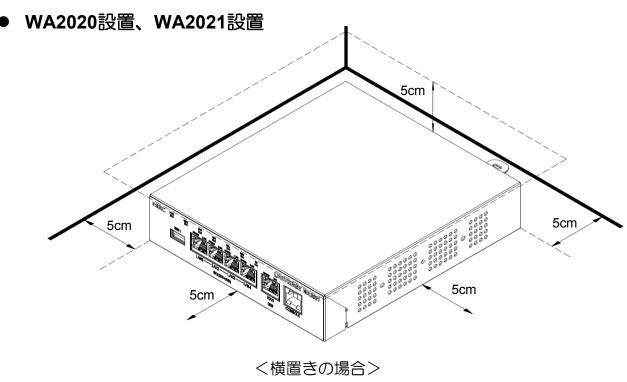
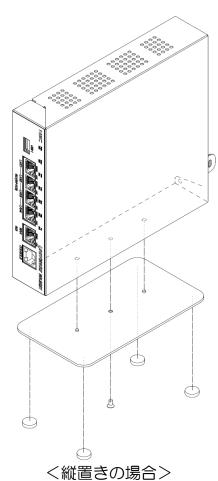
● **WA1020設置**

＜横置きの場合＞

＜縦置きの場合＞

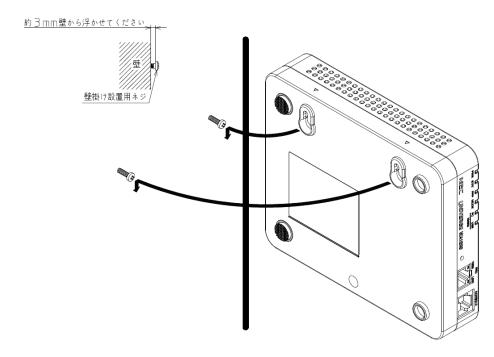
- **WA1510設置、WA1511設置**

＜横置きの場合＞

＜縦置きの場合＞

- **WA2020設置、WA2021設置**

＜横置きの場合＞

＜縦置きの場合＞

スタンドの凸部を製品の側面穴にあわせてネジで固定し、ゴム足を貼り付けて設置してください。

- **WA1020壁掛け設置**

注意　WA2020、WA2021は壁掛け設置には対応しておりません。

■壁掛けに使用するネジについて

付属のネジは、以下の仕様です。

ネジ頭　：ナベ頭

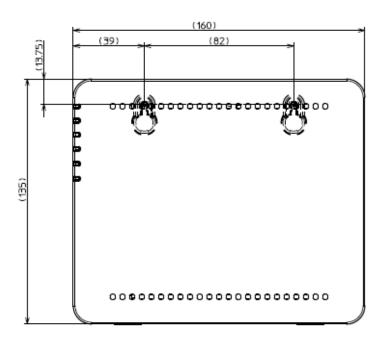
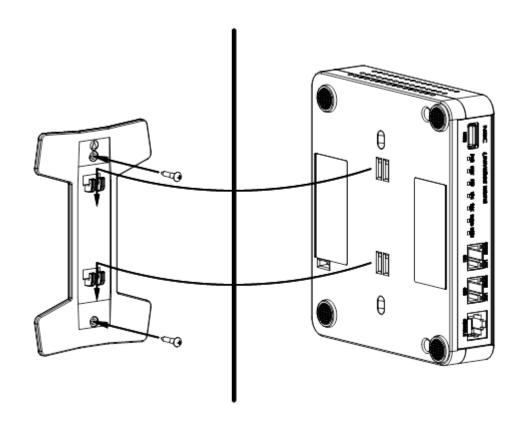
ネジ径　：M3.1

ネジ長さ:16mm 程度

素材　　:鉄

壁の素材、厚さ、強度等により、付属のネジでは、使用できない場合、購入時に購入先に確認してください。

右記にネジの間隔（82mm）を示しておりますが、壁掛け用の溝の上面に刻印（上図の▽印）があります。

この刻印にあわせて、壁に記しをつけるとメジャー等で測量しなくても簡単にネジ間隔を壁に表示できます。

● WA1510、WA1511壁掛け設置

■壁掛けに使用するネジについて

付属のネジは、以下の仕様です。
ネジ頭 ：ナベ頭
ネジ径 ：M3.1
ネジ長さ:16mm 程度
素材 :鉄

壁の素材、厚さ、強度等により、付属のネジでは、使用できない場合、購入時に購入先に確認してください。
壁掛け用の板を刻印（上図の△印）で上下の向きを合わせて壁面に当ててネジを取り付けてください。

設置環境

■データ通信端末使用時の設置環境について

本製品は、データ通信端末を接続して電波を利用した無線通信を行います。
そのため、ご利用になるデータ通信端末への電波が届く範囲内に設置が必要となります。
電波が届きにくい場所に設置しますと、通信が途切れたり、データ通信端末での接続が切れたりなど、電波状況等により通信が不安定になる可能性があります。また、電波が届く範囲内に設置されても、電波状況や他の利用者数の状況、アクセスポイントの状況等の状況によりつながりにくい場合があります。

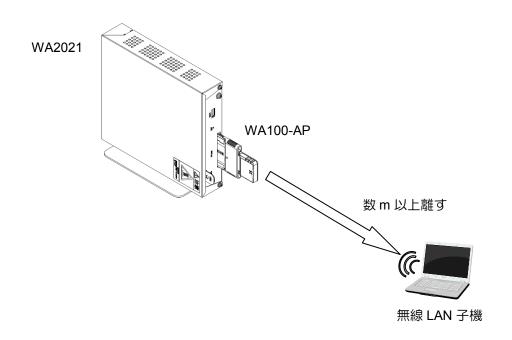
電波状況等につきましては、利用されるデータ通信端末の通信事業者様のサービスエリアをご確認の上、通信事業者様にお問合せください。

設置は、横置き、縦置き、壁掛け等に対応していますので、出来るだけ電波状況のよい環境に設置することをお勧めいたします。ただし壁掛け設置は、WA1020、WA1510、WA1511が対応しています。

WA 1511にてオプションアンテナを使用する場合は、アンテナ部分をねじ、両面テープ、マグネットシートでの固定に対応しています。出来るだけ電波状況のよい位置に設置することをお勧めいたします。

■無線 LAN 使用時の推奨設置環境について

無線 LAN 通信は、周囲の電波環境および壁や周囲の設置物の配置等の影響を受けることで、通信速度が低下したり、通信が途切れる、通信エラーが発生するなどの通信品質が劣化する場合があります。本製品の無線 LAN 使用時の推奨設置環境を以下に示しますが、ご利用の環境に合わせ、出来るだけ電波状況のよい環境に設置してください。

- 本製品を縦置き、かつ背面(無線LANカードが設置されている面)を子機側に向け、本製品と子機間は見通しのよい状態で設置して下さい。
（遮蔽物等がある場合、その影響により通信速度が低下することがあります)
- 本製品と子機間は数m以上離して設置してください。　但し、距離が離れすぎても通信エラーが発生、もしくは通信速度が低下することがあります。
（本製品と子機が通信可能な距離は見通しのよい場所でおよそ 180m 程度です）
- 本製品を、電気製品・AV・OA機器など磁気を帯びているところや電磁波が発生している場所の近くに設置しないでください。
- 本製品を湿気または水気の多い場所に設置しないでください。

USB メモリについて

WA シリーズでは、外部ストレージとして、USB メモリのオプション品（T-512）を用意しています。以下に USB メモリについて説明します。

■USB メモリの接続

①**USB** メモリのキャップ取り外し

オプション品の USB メモリに接続しているキャップを外し、USB の type A コネクタを出します。キャップを紛失しない様に保管します。

②**USB** ポートへの接続

USB メモリのラベル貼り付け面を下にして、本製品の USB ポートへ根元までまっすぐに差し込みます。

注意 使用できるUSBメモリは、オプション品のみとなります。市販のUSBメモリは使用できません。

注意 USBコネクタの向きが逆だと接続できません。無理に差し込まないでください。また、向きが正しい場合でも差し込みにくい場合は、無理に差し込まないでください。コネクタ/ポートが破損する場合があります。

注意 USBメモリにストラップを接続している場合は、USBポートに荷重がかからない様にストラップの取り回しにご注意願います。

注意 WA2021はUSBポートが2つありますが、同時に2ポート使用することはできません。どちらか1ポートをご使用ください。

■USB メモリの取り外し

①**USB** メモリへのアクセス確認

本製品の PWR、STAT ランプを確認し、PWR：緑点滅、STAT 赤点滅していないことを確認します。

②**USB** ポートから取り外し

USB メモリの筐体をつかみ、まっすぐに引き抜きます。

注意 USBポートに接続したUSBメモリ内のファイルへアクセス中に、USBメモリを本製品から外したり、本製品の電源を切ったりすると、アクセス中のデータが壊れる可能性がありますので、ご注意ください。

USBデータ端末の固定

■固定具を使った固定について

USB ポートからデータ通信端末が簡単に抜けないよう固定するために、USB 抜け防止用固定具と USB 抜け防止用ケーブルバンドが添付されています。USB データ通信端末を固定する場合にお使いください。（全機種共通：WA1511 除く）

注意　ケーブルバンドを一度使用すると、取り外すにはニッパー等でカットする必要がございます。固定具とケーブルバンドによる固定は、セットアップが完了し、通信ができることを確認した後にご使用ください。

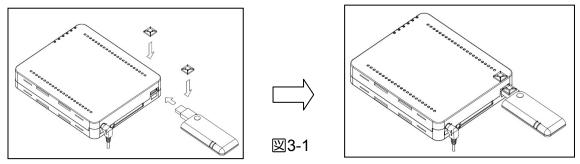
注意　USBデータ通信端末の形状によって、本固定具では十分な固定できない場合があります。

固定具·ケーブルバンドは以下の手順でご使用ください。(WA1020の例)

①固定具の貼り付け

固定具をUSBデータ通信端末と筐体上面にそれぞれ貼り付けます。

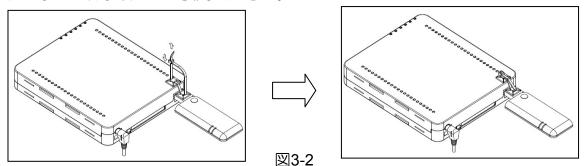
貼り付け位置は図3-1をご参照ください。

図3-1

注意　固定具は装置側とUSBデータ通信端末とで同じ面になるように近づけて貼り付けてください。なお、USBデータ通信端末の形状によっては貼り付けが出来ない場合がございます。

②ケーブルバンドの取り付け

図3-2に示すように、ケーブルバンドを取り付けてください。

バンドを強く引っ張りすぎると、USBコネクタ周辺が破損したり固定具が剥がれる場合がありますので、締め付ける際はご注意ください。締め付け後ケーブルの余長部分はハサミなどで切り取ってご使用ください。

図3-2

注意　USBデータ通信端末を取り外す際は、必ずニッパー等でケーブルバンドを切断してから行ってください。

■抜け防止金具を使用した固定について

USB ポートからデータ通信端末が簡単に抜けないよう固定するために、USB 抜け防止用金具とネジが添付されています。USB データ通信端末を固定する場合にお使いください。(WA2020、WA2021）

注意　USB抜け防止金具はUSB0ポートのみ（背面ポート）対応しております。装置前面のUSB1ポートで使用することはできません。

固定金具は以下の手順でご使用ください。

①固定金具の取り付け

データ通信端末をUSBポートに接続後、端末の取り付け方向を調整してください。

固定金具は、USBデータ通信端末の形状や取付け方向にあわせてネジで固定します。そのため、端末を接続する前に固定金具を取り付ける際は、固定金具をデータ通信端末にあわせてスライドできるようにネジを締めすぎないようにしてください。

固定金具の取り付け位置は、図3-3をご参照ください。

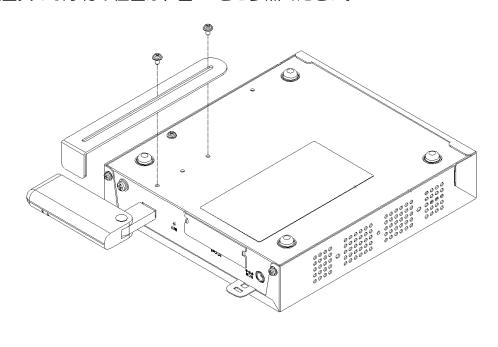
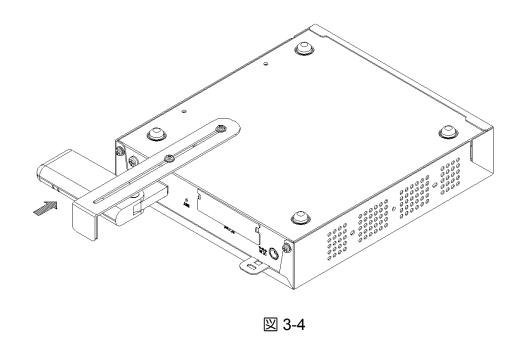



図 3-3

注意　固定用ネジ穴が3箇所ありますので、データ通信端末の形状に合わせて2箇所を選んで、ネジを2つ用いて固定してください。ネジで固定するまでは、金具がスライドしますのでご注意願います。

②データ通信端末の固定

図3-4に示すように、データ通信端末をUSBポートに接続して取り付け方向が決まりましたら、データ通信端末がUSBポートからはずれないように、固定金具をスライドさせL字型の部分で固定します。クッションがありますが、押さえすぎないようにします。金具がずれないように手で押さえながら、底面のネジを締めて固定します。

図 3-4

注意　固定金具はUSBポートからUSBデータ通信端末がはずれないように固定するものです。必要以上に圧迫するとUSBポート周辺が破損する恐れがありますので、ポートがゆるまない程度で固定してください。また、USBデータ通信端末の形状によってはうまく固定が出来ない場合がございます。

注意　USBデータ通信端末を取り外す際は、必ず固定金具を取り外してから行ってください。

内蔵モジュールについて（WA1511 のみ）

■内蔵モジュールの準備

内蔵モジュールを利用してモバイル回線に接続する場合は、内蔵モジュールに合わせたSIM カードを装置の背面にある SIM スライドカバーを開けて、SIM カードを正しい向きで取り付けます。また、アンテナ端子に専用のアンテナ 2 本を接続します。

注意　SIMカードは、標準SIMを使用します。マイクロSIM、ナノSIMは使用できません。

SIM スライドカバーを右にスライドさせると、SIM スロットが見えますので、ご利用の SIM を差し込んでください。

SIM カードの取り付け／取り外し

SIM 取り付け方法

- SIM スライドカバーを右にスライドさせます。
- SIM カードを図 3-5 に示す向きに挿入し、指で押して奥へ押し込んでください。

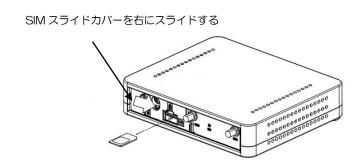



図 3-5

SIM 取り外し方法

・DC ジャックとセキュリティーロックを外します。（図 3-6）
・SIM カバースライドを右にスライドさせます。
・SIM の先端が見えますので指で軽く押して飛び出させて外してください。

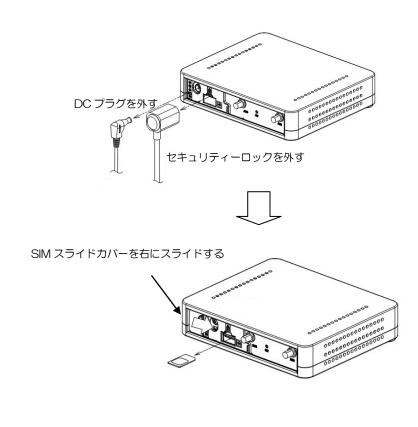



図 3-6

■アンテナについて

WA1511 では、添付のアンテナ及び電波環境の改善をサポートするためオプション品の延長アンテナを用意しています。以下にアンテナの接続について説明します。

同梱のアンテナや専用オプションのアンテナ以外は使用しないでください。

十分な通信の安定性・速度を確保するために必ず２本共接続してください。

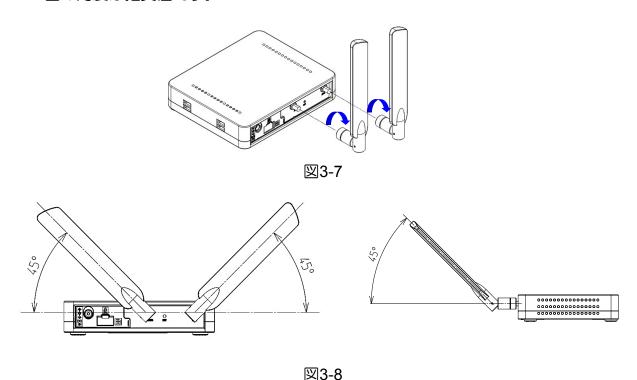
添付の直付けアンテナの接続

注意　アンテナ接続時に工具を使って力を加えると破損の危険があります。

① アンテナは接続部分をアンテナ用コネクタに挿入し、指でアンテナ接続部分（滑り止めが付いたアンテナ根本部分）を回して固定してください。
アンテナ本体を回しての取り付けは故障の原因になりますので行わないでください。（図3-7）

② 図3-8に示すように２本のアンテナが交差しないように設置してください。
お客様の環境に合わせて配置願います
図の角度は推奨値です。

図3-7

図3-8

注意　アンテナは金属などの導電性の物から離して設置してください。感度低下の可能性があります。
アンテナを軸方向に回転させすぎると内部で断線の可能性が生じます。
９０度以上回転させないようにしてください。

オプション品アンテナの接続

注意　必ず２本のアンテナを接続してご使用ください。

アンテナは以下の手順でご使用ください。

① アンテナケーブルの取り付け

アンテナのケーブルを本体のアンテナ端子に挿入し、指でナットを回して固定してください。（図3-9）

ペンチなどの工具を使う場合、締め付けすぎないように注意してください。（0.2Nm以内）

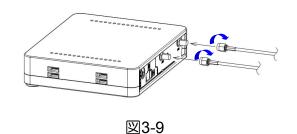
図3-9

注意　アンテナケーブルの弛みで本体が引きずられないように、アンテナケーブルを棚や机に固定してのご使用を推奨します。（図3-10）
ケーブル固定具は添付しておりませんのでお客様で準備お願いします。

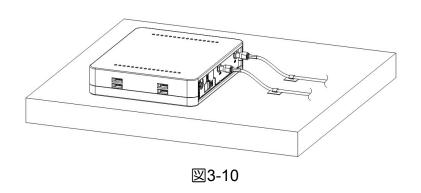
図3-10

② アンテナの固定

図3-11～13に示すように、2本のアンテナはネジ、もしくは添付の両面テープ、ラバーマグネットで固定してください。2本のアンテナの距離は30cm離して設置してください。アンテナは縦方向での設置を推奨します。
アンテナ固定用のネジはついておりませんので、設置場所の状況によりお客様でM4径のネジを準備お願いします。

ネジ固定の場合

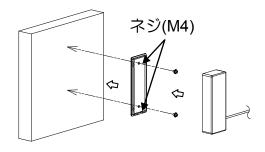



図 3-11

両面テープ固定の場合

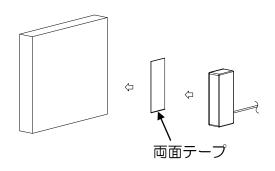



図 3-12

ラバーマグネットで固定の場合

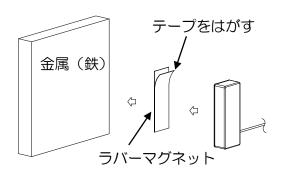



図 3-13

注意　アンテナは屋外設置可能ですが、できるだけ直射日光や雨が当たる場所を避けて設置してください。
屋外ではネジでの設置としてください。両面テープやラバーマグネットでの設置はできません。
また、アンテナ本体が水没している状態や、雪に覆われた状態では通信できません。

注意　アンテナの使用温度は-20℃～90℃です。両面テープ・ラバーマグネットで固定の場合は上限が80℃までとなります。

注意　アンテナケーブルの折り曲げ半径は50mm以上としてください。

注意　アンテナケーブルを固定する場合変形しないようにしてください。図3-14に示すように変形した状態では特性が劣化する可能性があります。

図 3-14

接続手順

■接続手順

以下の手順で、本製品とケーブル、通信端末、電源アダプタなどを接続します。

① 設置場所の確認
② SIMカード取り付け、アンテナ接続（WA1511の場合）
③ コンソールケーブルの接続
④ WAN側イーサネットケーブルの接続
(WA1510、WA1511、WA2020、WA2021使用時)
⑤ データ通信端末の接続
（WA1510、WA2020、WA2021の場合、必要に応じて）
⑥ LAN側イーサネットケーブルの接続
⑦ 無線LANカードの接続（WA2021の場合、必要に応じて）
⑧ ACアダプタを本体へ接続
⑨ ACプラグをACコンセントから差し込む事による起動

①設置場所の確認

設置場所が適切か確認します。

②SIM カード取り付け、アンテナ接続（WA1511）

背面のスライドカバーを右にずらし、SIMスロットにSIMカードを取り付けてください。

アンテナをアンテナ端子に接続してください。詳細な接続方法は、「本章 内蔵モジュールについて」をご確認ください。

注意 内蔵モジュールが対応している通信事業者のSIMカードを取り付けてください。内蔵モジュールの対応事業者は、販売元にご確認お願いします。
対応していない事業者のSIMカードを使用した場合は、正しく動作しません。

注意 SIMカードの活線挿抜はサポートしておりませんので、電源OFFの状態でSIMカードの取り付けを行なってください

注意 アンテナは、2本一組です。必ず2本とも接続してください。

注意 同梱のアンテナもしくは、専用オプションのアンテナ以外接続しないでください。

注意 WA1511で、USB接続のデータ通信端末を使用することはできません。

③コンソールケーブルの接続（コンソールによる設定を行う場合のみ）

コンソールポートに、付属のコンソールケーブル（RJ-45側）をカチッと音がするまで差し込んでください。

誤って、イーサネット(FE0,GE0,GE1)ポートに接続しないように注意してください。
（コンソールポートにランプはありません。）

コンソールケーブルの反対側をPC等のローカルコンソールに接続し、固定ネジを確実に締めてください。

注意 添付のコンソールケーブル以外のケーブルを接続しないでください。故障、焼損の原因となるおそれがあります。

注意 ローカルコンソールから、本製品の設定を変更する等以外で、特に使用することがないときは必ずコンソールポートからコンソールケーブルを抜いてください。

④WAN 側イーサネットケーブルの接続（WA1510、WA1511、WA2020、WA2021）

GE0ポートに、イーサネットケーブルをカチッと音がするまで差し込んでください。誤ってコンソールケーブルに接続しないように注意してください。

イーサネットケーブルの片端はWAN側の機器に接続してください。

注意 ケーブルを抜くときは、コネクタを持ち、ツメをつまんでまっすぐに引き抜いてください。

注意 イーサネットケーブル以外のケーブルを接続しないでください。故障、焼損の原因となるおそれがあります。

⑤データ通信端末の接続

USBポートまたはPCカードスロットにデータ通信端末を接続してください。

注意 サポートされているデータ通信端末以外は接続しないでください。

注意 USBハブ経由での接続はできません。

注意 データ通信端末の活線挿抜はサポートしておりませんので、電源OFFの状態でデータ通信端末の挿抜を行なってください。

注意 WiMAXとWiMAX以外のデータ通信端末を同時に接続することができます。ただし同時に使用できるデータ通信端末は２台までです。また、WiMAX同士、またはWiMAX以外のデータ通信端末同士のデータ通信端末を同時に使用することはできません。WA1510、WA1511ではWiMAXデータ通信端末は、サポートしておりません。

注意 WA2021で、無線LANカードとWiMAXデータ通信端末を同時に使用することはできません。

⑥イーサネットケーブルの接続

FE0ポート（WA1510、WA1511、WA2020、WA2021の場合はGE1ポート）に、イーサネットケーブルをカチッと音がするまで差し込んでください。
誤って、コンソールポートに接続しないように注意してください。

もう一方は、LAN側のルータやスイッチングハブ等に接続してください。

注意 ケーブルを抜くときは、コネクタを持ち、ツメをつまんでまっすぐに引き抜いてください。

注意 イーサネットケーブル以外のケーブルを接続しないでください。故障、焼損の原因となるおそれがあります。

注意 WA1020のFE0ポートを通信事業者が提供するWAN環境、回線終端装置に接続しないで下さい。

⑦無線 LAN カードの接続

PCカードスロットにオプション品の無線LANカード「WA100-AP」を接続してください。

注意　無線LAN機能は、WA2021とWA100-APの組合せでのみ動作します。WA100-AP以外の無線LANカードを使用しないでください。

注意　無線LANカード接続は、無線LANカードの取扱説明書を参照してください。

注意　無線LANカード WA100-APの活線挿抜はサポートしておりませんので、電源OFFの状態で挿抜を行なってください。

⑧AC アダプタを本体へ接続

ACアダプタのACプラグがACコンセントに差し込まれていない事を確認してから、ACアダプタのDCプラグを本体に接続します。

注意　DCプラグを接続するときや、取り外すときは、必ずコネクタを持って行ってください。またWA1510、WA1511、WA2020、WA2021の場合、ACアダプタと電源ケーブルが確実に接続されていることを確認してください。

⑨AC アダプタを AC コンセントに差し込む事による起動

接続が正しく行われたか確認し、ACアダプタをACコンセントに接続します。

製品の自己診断が行われます。

診断結果が正常（WA1020はSTATランプが赤点灯後、消灯へ変化し、その後緑点灯します。WA1510、WA1511、WA2020、WA2021は全LEDが点灯後、消灯へ変化し、その後STATランプが緑点灯します。）であることを確認します。

製品が自己診断で異常を検出した場合（STATランプが5秒ほど赤点灯し、消灯してまた赤点灯を繰り返し続けます。）は、販売元にご連絡ください。

注意　電源をOFFする場合、ACアダプタをACコンセントに接続した状態のまま、装置本体側のDCジャックを抜かないでください。必ずACプラグをコンセントから抜いてください。

設定インタフェース

本製品は、コマンドラインインタフェース(CLI)を利用した場合とWWWブラウザを利用した場合のどちらからも設定を行うことができます。

■コマンドラインインタフェースを利用した設定インタフェース

以下に示す、インタフェースより設定を行うことが出来ます。

ローカルコンソール

VTターミナル等コンソールによるアクセスで「コマンドラインインタフェース(CLI)」使用による詳細な設定や情報／状態確認が可能です。

リモートコンソール

リモートコンソールとしてtelnet/SSHが使用可能です。
リモートコンソールを使用するためには本製品にIPアドレスが設定され、telnetサーバ/SSHサーバ機能を開始しておく必要があります。

telnetサーバ/SSHサーバ機能に関する設定は、コマンドリファレンスをご参照ください。

■WWW ブラウザを利用した設定インタフェース

パソコンのWWWブラウザから、本製品のWeb-GUIへログインすることができます。

Web-GUIは、コマンドラインインタフェースに用いる設定コマンドを使用することなく、簡易に設定を行うことができます。

Web-GUIからの操作では、主な機能の設定が可能ですが、詳細な設定が必要な場合にはコマンドラインインタフェースからの設定をご使用ください。

Web-GUIの詳細は、Web-GUIマニュアルをご参照ください。

注意　コマンドラインインタフェースを用いて設定した場合、Web-GUIを用いて設定を変更することはできません。

工場出荷時設定

本製品の、初期導入時に使用する主な設定の工場出荷時設定は以下になっています。

■ユーザ名、パスワード

CLI ローカルコンソール／リモートコンソール用のアドミニストレータ権限、および Web-GUI 用のアドミニストレータ権限は以下です。

- ユーザ名　：**admin**
- パスワード　：**admin**

メモ ローカルコンソール／リモートコンソールのログインタイマは 0(秒) です。コンソールの操作が無くてもログアウトしません。

■IP アドレス

各製品には管理コンソール用として以下の IP アドレスが付与されています。

- IPアドレス：**192.168.1.200/24**

各製品の以下インタフェースに設定されています。

- WA1020　：FastEthernet0.0
- WA1510、WA1511　：GigaEthernet1.0
- WA2020、WA2021　：GigaEthernet1.0

メモ WA1020はDHCPサーバ機能が無効になっています。
WA1510/WA1511、WA2020、WA2021はDHCPサーバ機能が有効になっています。

メモ WA2020はソフトウェアバージョン4.2以降で対応しています。

■WA1020 動作モード

- アダプタモード

■Web-GUI 初期 URL

Web-GUI へログインするための初期 URL は以下です。IP アドレスが設定されているポートに管理用端末を接続してください。

- **https://192.168.1.200/**

メモ Web-GUI詳細についてはWeb-GUIマニュアルをご参照ください。

無線LANカードについて

■無線 LAN カード　サポート機種について

WA2021 で無線 LAN アクセスポイント機能を使用する場合は、以下の無線 LAN カードをご使用ください。

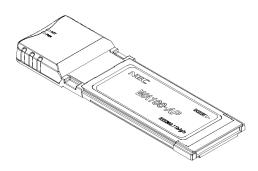
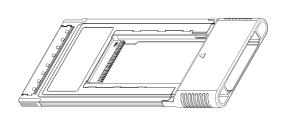
2012年7月時点での無線LANカードのサポート機種は以下となります。

- WA100-AP ・・・ UNIVERGE WA2021　オプション品

■WA100-AP について

無線 LAN カード「WA100-AP」は、UNIVERGE WA2021 専用の無線 LAN カードです。

「WA100-AP」は、ExpressCard タイプ無線 LAN カード本体「WA100-WE」と PC Card/ExpressCard 変換アダプタ「WA100-AD」のセット品です。

□WA-100WE （無線 LAN カード本体）　　□WA100-AD （PC カードアダプタ）

注意　WA100-APご使用にあたっては、無線LANカードの取扱説明書をご確認ください。

注意　「WA100-WE」のみでご使用することはできません。必ず「WA100-AD」に取り付けてご使用ください。

注意　「WA100-WE」と「WA100-AD」の単体販売はしておりません。

■WiMAX データ通信端末と無線 LAN カードの併用について

WA2021において、WiMAXデータ通信端末とWA100-AP無線LANカードは、併用することはできません。WiMAXデータ通信端末とWA100-AP無線LANカードを同時に接続すると、WiMAXデータ通信端末は無効になり、WA100-AP無線LANカードのみが有効になります。

4

基本操作と設定

4-1
基本操作と各種説明

コマンド入力について

本製品の設定方法は、ローカルコンソール／リモートコンソールで利用されるCLI (コマンドラインインタフェース)と、WWWブラウザ利用の2通りの方法があります。

本章では、ローカルコンソール／リモートコンソールで利用されるCLIによる基本操作について記載しています。

WWWブラウザによる設定の詳細は、Web-GUIマニュアルをご参照ください。

■コマンドについて

本製品は、CLIでコマンドを受け付けます。

コマンドは、表示されているプロンプトに続けて、1つのコマンドをスペースで区切って入力します。

また、パラメータが必要なコマンドも、コマンドとの間をスペースで区切って入力します。

入力は、1バイト文字（半角）の英数字、記号で行います。一部のコマンド（ログイン、パスワード等）を除いて、大文字、小文字の区別はありません。

工場出荷時は装置によってプロンプトのホスト名部分の表示が異なります。WA1020の場合は「WA1020」と、WA1510、WA1511の場合は「WA1500」と、WA2020の場合は「WA2020」と、WA2021の場合は「WA2021」と表示されます。以下はWA1020の場合を代表例として記載しますので、装置によってコマンドプロンプトの表示は読み替えてご参照ください。

■コマンド入力時のエラーメッセージ

コマンドが間違っていたり、ユーザ権限で認められていないコマンドの場合は、以下のようなエラーメッセージを出力します。

```
WA1020# aa
% aa  -- Invalid command.
WA1020#
```

キー操作と画面表示について

コマンド入力時には、カーソル移動、文字の削除、補完、ヘルプ機能を使用できます。

■カーソル移動

コマンドライン上で、カーソルを左右に移動することができます。

[CTRL]+b、または←	１文字（カーソルの左）に移動します。
[CTRL]+f、または→	１文字（カーソルの右）に移動します。
[CTRL]+a	行の先頭へジャンプします。
[CTRL]+e	行の終わりへジャンプします。

```
WA1020# configure
                        [CTRL]+b 、または ←（ 1 文字左へ）
WA1020# configure
                        [CTRL]+a （行の先頭へ）
WA1020# configure
                        [CTRL]+f 、または →（ 1 文字右へ）
WA1020# configure
                        [CTRL]+e （行の終わりへ）
WA1020# configure
```

■コマンドラインの文字編集

カーソル移動と併用することで、コマンドライン上の文字を削除、編集することが可能です。

[Back Space]	カーソルの左の1文字を削除します。
[CTRL]+d	カーソル位置の文字を1文字削除します。
[CTRL]+k	カーソル位置から行末まで削除します。
[CTRL]+c	コマンドラインの文字をすべて削除します。

```
WA1020# cnofofigure
                [CTRL]+d   （カーソル位置の 1 文字「f」を削除）
WA1020# cnoofigure
                [Back Space]   （カーソルの左の 1 文字「o」を削除）
WA1020# configure
                [CTRL]+k   （カーソル位置から行末まで削除）
WA1020# co
                [CTRL]+c   （文字をすべて削除）
WA1020#
```

■投入済みコマンドの呼び出し

キー操作により、今までに投入したコマンドを呼び出すことができます。

最後に入力したコマンドから新しい順に9個前まで呼び出すことができます。

バッファのすべての履歴コマンドを一巡すると、プロンプトのままとなります。

呼び出したコマンドは、文字編集が可能です。

メモ　再起動すると、コマンド履歴は削除されます。

[CTRL]+p、または↑	前に入力されたコマンドを新しい順から呼び出します。
[CTRL]+n、または↓	前に入力されたコマンドを古い順から呼び出します。

起動後、3つのコマンドを「exit」⇒「telnet」⇒「save」の順に入力していた場合、以下に示す順序で呼び出すことができます。

組み合わせて使用した場合は、現在表示されているコマンドからの相対的な順となります。

```
WA1020#
                    [CTRL]+p、または↑
WA1020# save
                    [CTRL]+p、または↑
WA1020# telnet
                    [CTRL]+n、または↓
WA1020# save
                    [CTRL]+n、または↓
WA1020#
```

■コマンドの補完

[TAB]キーにより、数文字を入力しただけで完全な形のコマンドに補完することができます。

入力した文字列で始まるコマンドが１つだけの場合、[TAB]キーを押すとそのコマンドの残りの文字列が補完されます。

```
WA1020# conf [TAB]
WA1020# configure
```

メモ　入力した文字列で始まるコマンドが複数ある場合に[TAB]キーを押すと、コマンドは補完されません。入力途中の文字列で始まる補完可能なコマンドが表示されます。

```
WA1020# cl [TAB]
   clear              -- clear entry
   clock              -- set date and time
WA1020# cl
```

■コマンドの省略入力

入力した文字列で始まるコマンドが1つだけの場合、そのまま[Enter]キーでコマンドを投入することができます。

```
WA1020# conf [Enter]
WA1020(config)#
```

また、複数の単語を組み合わせたコマンドの場合も、それぞれの単語が省略可能であれば、単語毎の省略入力が可能です。

単語の間はスペースで区切ります。

例はshow interfaces detail コマンドを省略して投入しています。

```
WA1020(config)# sh int de [Enter]
                （省略）
WA1020(config)#
```

■ヘルプ機能

[?]キーにより、コマンドの説明一覧を表示することが可能です。

[?]キーを押すと、その状態で利用可能なコマンドまたはパラメータの説明が表示されます。

```
WA1020(config-FastEthernet0.0)# ip address  ?
  A.B.C.D/<0-32> -- IP address
WA1020(config-FastEthernet0.0)# ip address
```

メモ　[TAB]キーをヘルプ機能として代用することも可能です。ただし、あくまでも[TAB]キーは補完機能キーですので、候補が1つしかない場合には、説明表示ではなく、コマンドを補完します。

■画面表示

行数の多い情報が表示される場合は、表示の途中で「--More--」が表示されます。次の数行を表示する場合は[SPACE]キーを、1行ずつ表示していく場合は[Enter]キーを押します。また、[Q]キーを押すと続きの表示を中止し、プロンプトを表示します。

```
--More--
```

■コマンド入力の注意点

コマンド入力においては、以下の注意点があります。

制御文字列を含まないアスキー文字列の使用

コマンド入力においては、アスキー文字を使用してください。

コンソールのモードについて

■モード構成

本製品のモードには、オペレーションモード、制限オペレーションモード、特権モード、コンフィグモードの4つのモードがあります。また、コンフィグモードには、2つのモードがあります。

- オペレーションモード‥‥‥‥‥‥‥ログイン後、最初に入るモードです。
導通確認（ping、traceroute）や装置情報の確認などができます。
プロンプトは「>」(hostname>)で表示されます。
- 制限オペレーションモード‥‥‥‥‥ほかのユーザが先にログインしている時に入るモードです。
装置情報の確認ができます。
プロンプトは「$」(hostname$)で表示されます。
- 特権モード‥‥‥‥‥‥‥‥‥‥‥‥設定保存や統計情報のclear、データ通信端末でのISP接続や切断、再立ち上げ(reboot)、装置設定情報の確認などができます。
プロンプトは「#」(hostname#)で表示されます。
- コンフィグモード
  - グローバルコンフィグモード‥‥一般的な設定を行うモードです。
  - サブコンフィグモード‥‥‥‥‥各ポートや物理ポートの動作設定を行うモードです。

それぞれのコマンドには対応したモードがあり、そのモードに移ってから入力可能となります。

モード状態遷移詳細については、コマンドリファレンス付録「モード遷移」をご参照ください。

メモ　上記以外に、ブートモニタがあります。通常の作業ではこのブートモニタに入ることはありませんが、障害発生時や緊急時の本製品の保守で使用します。

■オペレーションモードと特権モード間でのモード変更

オペレーションモードから特権モードへ

オペレーションモードから特権モードには、enableコマンドで移ります。コンフィグモードに移ると、プロンプト表示も変わります。

```
WA1020> enable [Enter]
WA1020#
```

注意　オペレーションモードから直接コンフィグモードやサブコンフィグモードを指定して移ることはできません。

特権モードからオペレーションモードへ

特権モードからオペレーションモードには、[Ctrl]＋ｚで移ります。

```
WA1020#  [Ctrl]+z
WA1020>
```

または、exitコマンドでも移ることができます。

```
WA1020#  exit [Enter]
WA1020>
```

■制限オペレーションモードからオペレーションモードへのモード変更

制限オペレーションモードからオペレーションモードへは、forced-adminコマンドで移ります。

```
WA1020 console

login: admin [Enter]
Password:***** [Enter]
Copyright (c) NEC Platforms, Ltd. 2009-2012 All rights reserved.
Copyright (c) 1996-2004
   The NetBSD Foundation, Inc.  All rights reserved.
Copyright (c) 1982, 1986, 1989, 1991, 1993
   The Regents of the University of California.  All rights reserved.
% Access Denied
WA1020$          ←―――――――――――――――――――― 制限オペレーションモード

WA1020$ forced-admin [Enter]
Enter configuration commands, one per line. End with CNTL/Z.
WA1020>          ←―――――――――――――――――――― オペレーションモード
```

注意　forced-adminコマンドを入力すると、１人目のログインユーザは、強制的にログアウトされます。

■特権モードとコンフィグモード間でのモード変更

特権モードからコンフィグモードへ

特権モードからコンフィグモードには、configureコマンドで移ります。コンフィグモードに移ると、プロンプト表示も変わります。

```
WA1020# configure [Enter]
WA1020(config)#
```

メモ　オペレーションモードからコンフィグモードに移ったときは、グローバルコンフィグモードになります。

注意　特権モードから直接サブコンフィグモードを指定して移ることはできません。

コンフィグモードから特権モードへ

コンフィグモードから特権モードには、[Ctrl]＋ｚで移ります。

```
WA1020(config)#  [Ctrl]+z
WA1020#
```

または、exitコマンドでも移ることができます。

```
WA1020(config)#  exit [Enter]
WA1020#
```

サブコンフィグモードから特権モードへ

[Ctrl]＋ｚで特権モードに移ることができます。

```
WA1020(config-FastEthernet0.0)#  [Ctrl]+z

WA1020#
```

■コンフィグモード内でのモード変更

グローバルコンフィグモードからサブコンフィグモードへ

グローバルコンフィグモードからインタフェースまたは他のサブコンフィグモードへは、設定対象とする個別インタフェースまたは機能を指定してそれぞれのモードに移ります。

```
WA1020(config)# interface FastEthernet0.0 [Enter]
WA1020(config-FastEthernet0.0)#
```

サブコンフィグモードからグローバルコンフィグモードへ

サブコンフィグモードからグローバルコンフィグモードへは、exitコマンドで移ります。

```
WA1020(config-FastEthernet0.0)#  exit [Enter]

WA1020(config)#
```

■オペレーションモード、制限オペレーションモードからログイン認証へ（ログアウト）

ログアウトは、exitコマンドで行います。

```
WA1020>exit [Enter]
login:
```

```
WA1020$exit [Enter]
login:
```

■インタフェース表示の意味

本製品のインタフェースの表示は、それぞれ以下の内容を示しています。

- FastEthernet0.0　FE0ポートです。アダプタモードではVPNルータを接続し、ルータモードではLAN接続機器（PC、HUB等）を接続します。WA1020でのみ表示されます。
- FastEthernet1.0　WiMAX用データ通信端末動作時に、WiMAX接続用として動作するインタフェースです。端末が未接続の場合は、表示されません。ルータモードの場合は、プロバイダから取得したIPアドレスが設定されます。
- GigaEthernet0.0　GE0ポートです。WAN機器（光モデム、ADSLモデムなど）を接続します。WA1510、WA1511、WA2020、WA2021で表示されます。
- GigaEthernet1.0　GE1ポートです。LAN機器（PC、HUB等）を接続します。WA1510、WA1511、WA2020、WA2021で表示されます。
- Serial0　3G/3.5G/LTE/PHSのデータ通信端末または内蔵モジュールと通信するためのインタフェースです。
データ通信端末または内蔵モジュールとやり取りする設定を行います。
ルータモードの場合は、プロバイダから取得したIPアドレスが設定されます。
- MobileEthernet0.0　3G/3.5G/LTEのデータ通信端末または内蔵モジュールと通信するためのインタフェースです。NDIS接続(※)にて通信します。
データ通信端末または内蔵モジュールとやり取りする設定を行います。
ルータモードの場合は、プロバイダから取得したIPアドレスが設定されます。
- Loopback0.0　内部に仮想的にインタフェースを設定する場合に使用します。
- Loopback1.0　内部に仮想的にインタフェースを設定する場合に使用します。WA1510、WA1511、WA2020、WA2021で表示されます。
- IPsec[＊]　IPsecをトンネルモードで通信する場合に使用します。
トンネル用のインタフェースとなります。
WA1020は2個、WA1510、WA1511、WA2020、WA2021は最大8個までインタフェースの追加が可能です。
- EtherIP0　EtherIPで通信する場合に使用します。EtherIPカプセル用の仮想インタフェースとなります。
- PPPoE[＊]　PPPoEで通信する場合に使用します。最大4セッション分までインタフェースの追加が可能です。WA1510、WA1511、WA2020、WA2021で表示されます。
- VLAN[＊]　VLANで通信する場合に使用します。ポートVLANの場合は最大4個タグVLANの場合は最大16個までインタフェースの追加が可能です。
ポートVLANは、WA2020、WA2021でサポートします。

- WirelessEthernet[＊] 無線LAN子機と通信するためのインタフェースです。最大4個のSSIDに対応したインタフェースの追加が可能です。
  無線LAN機能はWA2021のみでサポートします。
- L2TP[＊] L2TPv3で通信する場合に使用します。L2TPv3カプセル用の仮想インタフェースとなります。最大2個までインタフェースの追加が可能です。

[＊] ：インタフェース番号を示します。

(※)NDIS接続：Network Driver Interface Specificationに準拠したネットワークアダプタ接続方式です。

ログインとユーザ権限

■ユーザ権限について

本製品には、2種類のユーザ権限が用意されています。

アドミニストレータ‥ すべてのコマンドを実行することができます。

オペレータ‥‥‥‥‥ 設定を変更するコマンドは実行できませんが、設定情報や製品構成情報の表示、統計情報の表示と削除を実行することができます。

どちらのユーザ権限でログインしているかは、コマンドプロンプト表示では明示されません。

オペレータ権限の場合、特権モードに移ることはできません。

ログイン時

オペレータ及びアドミニストレータモードでログインした場合でも、プロンプトが「>」表示となります。

```
WA1020>
```

アドミニストレータ権限の場合

特権モードに移行した場合は、プロンプトが「#」表示となります。

```
WA1020> en [Enter]
WA1020#
```

オペレータ権限の場合

特権モードに移行しようとした場合は、エラーメッセージが表示されます。

```
WA1020> en [Enter]
% en  -- Access not permitted.
WA1020>
```

■ユーザ登録とユーザ権限の設定

ユーザ登録とユーザ権限の設定は、グローバルコンフィグモードでusernameコマンドを使用して行います。

例では、ユーザ名「WA1020-operator」、パスワード「abcd123」、ユーザ権限「オペレータ」でユーザ登録しています。アドミニストレータ権限のユーザを登録する場合には、パラメータにadministrator を使用します。

ユーザ名は最大16文字までです。パスワードは最大128文字までです。

注意　パスワードは、他の人が予想しにくい文字、数字の組み合わせにしてください。

```
WA1020(config)# username WA1020-operator password plain abcd123 operator [Enter]
% User 'WA1020-operator' has been added.
WA1020(config)#
```

メモ　ソフトウェアバージョン5.1.3までは、すでに登録されているユーザ名を入力しようとすると、以下のようにエラーメッセージが表示されます。

```
WA1020(config)# username WA1020-operator password plain abcd123 operator [Enter]
% input username is already registered.
WA1020(config)#
```

■ユーザの削除

登録したユーザを削除することができます。

削除は、グローバルコンフィグモードでno usernameコマンドを使用して行います。

```
WA1020(config)# no username WA1020-admin  [Enter]
% User 'WA1020-admin' has been deleted.
WA1020(config)#
```

注意　セキュリティのため、アドミニストレータ権限のユーザは、全部削除できません。最低1つは残ります。工場出荷設定のユーザを削除するには、先に追加登録が必要です。ご注意ください。

■ログイン

アドミニストレータ権限のユーザ登録がある場合には、起動時や、リモートコンソールからのアクセス時にはログイン認証が行われます。登録したユーザ名とパスワードでログインします。

例では、ユーザ名「WA1020-admin」、パスワード「abcd123」、ユーザ権限「アドミニストレータ」でログインしています。

```
login: WA1020-admin  [Enter]
Password: abcd123 [Enter]
Copyright (c) NEC Platforms, Ltd. 2009-2014 All rights reserved.
Copyright (c) 1996-2004
    The NetBSD Foundation, Inc.  All rights reserved.
Copyright (c) 1982, 1986, 1989, 1991, 1993
    The Regents of the University of California.  All rights reserved.
Enter configuration commands, one per line. End with CNTL/Z.
WA1020>
```

実際の画面では、入力したパスワードは画面上に表示されません。

■複数ユーザのログインについて

ソフトウェアバージョンにより、複数ユーザのログイン条件が異なります。

- ソフトウェアバージョン **4.3.13以降**

本装置へログイン可能なユーザ数は１人ですが、権限に関わらず、制限オペレーションモードに複数ユーザがログイン可能です。１人目のユーザがログインしている時は、２人目以降のユーザは自動的に制限オペレーションモードへのログインとなります。制限オペレーションモードへ同時にログインできる最大数は２０ユーザです。
forced-adminコマンドを入力することで、１人目のログインユーザを強制的にログアウトさせ、オペレーションモードへログインすることができます。

制限オペレーションモードでは、以下のコマンドが実行可能です。

exit
forced-admin
no
show
terminal

制限オペレーションモードのプロンプトは「$」で表示されます。

- ソフトウェアバージョン **4.0.0～4.3.6**

本装置へログイン可能なユーザ数は１人ですが、アドミニストレータ権限のユーザのみ、制限オペレーションモードに複数ユーザがログイン可能です。オペレーション権限のユーザは、１人目のユーザがログインしている時は、いずれのモードにもログインすることはできません。

制限オペレーションモードの同時ログイン数、forced-admin動作、および制限オペレーションモードで実行可能なコマンドは、ソフトウェアバージョン 4.3.13 以降と同じですが、プロンプトは「#」で表示されます。

- **ソフトウェアバージョン 3.2.x以前**

  ソフトウェアバージョン 4.0.0～4.3.6と同じです。

  但し、制限オペレーションモードでは、以下のコマンドのみ実行可能です。

  exit
  forced-admin

■タイムアウトによる強制ログアウト

コンフィグモードに入っていたユーザが、コマンド入力を一定時間行わないと、強制的にログアウトされ、そのユーザが使用していた端末には「login：」プロンプトが表示されます。タイムアウト時間は、terminal timeoutコマンドで設定できます。初期値は、強制タイムアウトは行わない設定(terminal timeout 0)です。

■Web-GUI のユーザについて

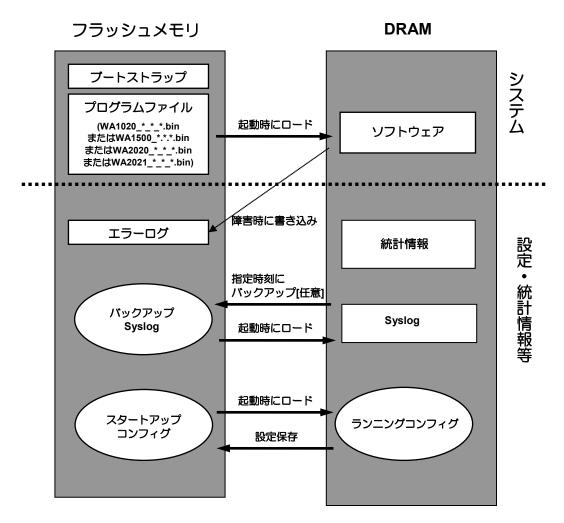
Web-GUIとCLIのユーザアカウントは、別々のコマンドによる管理となります。

CLIでログイン中に、Web-GUIでログインすると強制ログイン動作により、CLIはログアウトさせられます。

Web-GUI用のユーザアカウントの登録は、Web-GUIからだけでなくCLIからも可能です。

ソフトウェアと設定データ

■格納場所について

設定データやプログラム等の格納場所を下図に示します。

<u>フラッシュメモリ</u>

ブートストラップ、プログラムファイル、エラーログ、バックアップSyslog、スタートアップコンフィグが格納されています。

プログラムファイルとスタートアップコンフィグは、コマンドにより消去あるいはTFTPサーバとのファイル転送が可能です。

注意　フラッシュメモリへのアクセス中（STATランプ赤点滅中）に電源をOFFにすると、フラッシュメモリ内のファイル等を破壊することがあります。フラッシュメモリへのアクセス中は絶対に電源をOFFにしないでください。

DRAM

書き換え、消去が可能なメモリエリアで、電源がOFFになると全内容が消去されます。

プログラムファイル内のソフトウェアと、スタートアップコンフィグがフラッシュメモリからDRAMにロードされます。Syslogのバックアップ設定がされている場合は、バックアップSyslogもDRAMにロードされます。

ブートストラップ

電源がONになると最初に動作し、製品の自己診断やプログラムのロードなどを行うソフトウェアです。ブートファイルとテストプログラムで構成されています。また、プログラムファイルの異常などにより、プログラムのロードが中断された場合には、製品復旧用のモードである「ブートモニタ」に遷移します。

プログラムファイル

ソフトウェアを格納するファイルです。

プログラムファイルはフラッシュメモリ内に格納されており、本製品の起動時に

プログラムファイル内のソフトウェアがDRAMへロードされます。プログラムファイルは、show storageコマンドで表示されたリストの最上位から順番にロードします。

ソフトウェア

DRAM上で動作し、データ通信端末の動作や指定機能を処理するソフトウェアです。

エラーログ

製品の異常など障害発生時のログがフラッシュメモリ内のエラーログに書き込まれます。

統計情報

ソフトウェアが動作中に収集した統計情報のデータです。

SNMPによる統計情報の取得が可能です。

Syslog

Syslog設定がされている場合、イベント情報などのログがDRAM内に書き込まれます。

Syslogサーバ設定がされている場合、SyslogサーバへSyslogを転送します。

バックアップ Syslog

Syslogのバックアップ機能が設定されている場合、指定時刻にフラッシュメモリ内のバックアップSyslog領域に書き込まれ、本製品の起動時にはDRAM内のSyslog領域にロードされます。なお、書き込まれたSyslogを直接FTP/TFTP等で外部へ転送することはできません。

スタートアップコンフィグ

本製品の動作を決定する設定データ（コンフィグレーションファイル）です。

スタートアップコンフィグは本製品の起動時にDRAMにロードされます。

ランニングコンフィグ

本製品の動作を決定する設定データ（コンフィグレーションファイル）です。

本製品の起動直後はスタートアップコンフィグと同じ内容ですが、コマンドによる設定変更などを行うことで現在の製品動作を変更することができ、設定変更内容はランニングコンフィグに格納されます。

メモ　スタートアップコンフィグの内容を最新にしておくには、ランニングコンフィグを変更した後に、saveコマンドによりスタートアップコンフィグの内容をランニングコンフィグの内容に更新しておきます。

■起動順序について

電源がONになると、以下の順序で動作します。

①ブートストラップが動作し、製品の自己診断が行われます。

②boot entry コマンドにより、起動時のプログラムファイルが指定されていた場合、指定されたプログラムファイルをロードします。

注意　boot entry コマンドによるプログラムファイル指定がない場合、show storage コマンドで最上位に表示されているプログラムが選択されます。

③プログラムファイル内のソフトウェアを DRAM 上にロードし、ソフトウェアを起動します。

④スタートアップコンフィグを DRAM 上にランニングコンフィグとしてロードします。スタートアップコンフィグがない場合、工場出荷時の設定で起動します。

WA1020での画面例を以下に示します。

```
IPL: HARD-RESET
IPL: MEMORY OK

Boot: Version 2.1.0
POST:
DRAM Test ..... PASS
TClock Test ... PASS
FLASH CHKSUM .. PASS
LAN Test ..... PASS
PCI Test ..... PASS
USB Test .... PASS
3DES->HMAC-SHA1 TEST ... PASS
AES256->HMAC-SHA1 TEST ... PASS
DES->HMAC-MD5 TEST ... PASS
3DES->HMAC-MD5 TEST ... PASS
AES128->HMAC-MD5 TEST ... PASS
AES192->HMAC-MD5 TEST ... PASS
AES256->HMAC-MD5 TEST ... PASS
NULL->HMAC-MD5 TEST ... PASS
post success
LM: loading "wa1020.bin"
................................................................................
Thu Jan  1 00:00:07 JST 2009

WA1020 console

login:
```


メモ　reboot コマンドによる再起動の場合、設定されている時刻は保持されます。

WA1510/WA1511での画面例を以下に示します。

```
IPL: HARD-RESET
IPL: MEMORY OK
IPL: LOADING BOOT

Boot: Version: 1.0.1
POST:
FLASH CHKSUM .. PASS
DRAM TEST ..... PASS
RTC TEST ...... PASS
WAN TEST ..... PASS
LAN TEST ..... PASS
TEMP TEST .... PASS
3DES->HMAC-SHA1 TEST ... PASS
AES256->HMAC-SHA1 TEST ... PASS
3DES->HMAC-SHA2 TEST ... PASS
AES256->HMAC-SHA2 TEST ... PASS
DES->HMAC-MD5 TEST ... PASS
3DES->HMAC-MD5 TEST ... PASS
AES128->HMAC-MD5 TEST ... PASS
AES192->HMAC-MD5 TEST ... PASS
AES256->HMAC-MD5 TEST ... PASS
NULL->HMAC-MD5 TEST ... PASS
USB TEST .... PASS
post success
LM: loading "wa1500.bin"
.........................................................................................
..
Tue Jan  1 09:04:58 JST 2014

WA1500 console

login:
```

①製品基本部の自己診断
②③プログラムファイルのロード
④「login:」表示

WA2020での画面例を以下に示します。

```
IPL: HARD-RESET
IPL: MEMORY OK
IPL: LOADING BOOT

Boot: Version 1.0.1
POST:
DRAM Test ..... PASS
TClock Test ... PASS
RTC Test ...... PASS
FLASH CHKSUM .. PASS
WAN Test ..... PASS
LAN Test ..... PASS
PCI Test ..... PASS
3DES->HMAC-SHA1 TEST ... PASS
AES256->HMAC-SHA1 TEST ... PASS
DES->HMAC-MD5 TEST ... PASS
3DES->HMAC-MD5 TEST ... PASS
AES128->HMAC-MD5 TEST ... PASS
AES192->HMAC-MD5 TEST ... PASS
AES256->HMAC-MD5 TEST ... PASS
NULL->HMAC-MD5 TEST ... PASS
USB Test .... PASS
post success
LM: loading "wa2020.bin"
................................................
Thu Jan  6 14:24:12 JST 2011

WA2020 console

login:
```

WA2021 での画面例を以下に示します。

```
IPL: HARD-RESET
IPL: MEMORY OK
IPL: LOADING BOOT

Boot: Version 1.0.3
POST:
DRAM Test ..... PASS
TClock Test ... PASS
RTC Test ...... PASS
FLASH CHKSUM .. PASS
WAN Test ..... PASS
LAN Test ..... PASS
PCI Test ..... PASS
3DES->HMAC-SHA1 TEST ... PASS
AES256->HMAC-SHA1 TEST ... PASS
DES->HMAC-MD5 TEST ... PASS
3DES->HMAC-MD5 TEST ... PASS
AES128->HMAC-MD5 TEST ... PASS
AES192->HMAC-MD5 TEST ... PASS
AES256->HMAC-MD5 TEST ... PASS
NULL->HMAC-MD5 TEST ... PASS
USB Test .... PASS
post success
LM: loading "wa2021.bin"
.............................................
Tue May 24 10:20:30 JST 2012

WA2021 console

login:
```

データ通信を始める前に

■イーサネットのポート設定と通信について

①GE0 ポートの設定（WA1510、WA1511、WA2020、WA2021 の場合）

GE0ポートは、WAN接続用としてADSLモデム，ONUなどの回線終端装置に接続します。

プロバイダとの契約に合わせてPPPoE接続の設定、もしくはDHCPクライアント機能の設定を行ってください。

PPPoEで接続する場合は、PPPoEの仮想インタフェースを使用する必要があります。1セッション1インタフェースを使用し、同時セッション数に合わせて、PPPoE0からPPPoE3までの同時4セッション設定が可能です。GE0ポートでは割り当ての設定をしてください。

DHCPクライアント機能は、GE0ポートにてIPアドレス取得方法をDHCPに設定してください。

また、ポートの通信モードをauto設定で使用する場合は、対向ポートとの相性問題等がありますので、接続後に対向ポートと同じ通信モードでリンク確立しているかを確認してください。対向ポートの通信モードが一致しない場合、正しく通信できないおそれがありますので速度および半二重/全二重の通信モードを対向ポートと同じになるように固定設定をしてください。

②FE0/GE1 ポートの設定

WA1020ではFE0ポート、WA1510、WA1511、WA2020、WA2021ではGE1ポートの設定について説明します。

ポートの通信モードをauto設定で使用する場合は、対向ポートとの相性問題等がありますので、接続後に対向ポートと同じ通信モードでリンク確立しているかを確認してください。対向ポートの通信モードが一致しない場合、正しく通信できないおそれがありますので速度および半二重/全二重の通信モードを対向ポートと同じになるように固定設定をしてください。

注意　　FE0 ポートは、LAN 側の機器接続用として使用し、WAN 接続用としては使用しないでください。

■インタフェース Serial0 と MobileEthernet0.0 について

HSPA/LTE動作のデータ通信端末及び内蔵モジュールは、端末の仕様によりインタフェースSerial0またはインタフェースMobileEthernet0.0を選択して使用することができます。どちらか選択しての使用になりますので、MobileEthernet0.0インタフェースをno shutdownした場合、Serial0インタフェースは自動的にshutdownします。また、Serial0インタフェースを no shutdownした場合、MobileEthernet0.0インタフェースは自動的にshutdownします。以下に上記インタフェースの動作と設定を説明します。

●Serial0の動作概要

ダイヤルアップ方式を使用して、point to pointで網と接続します。PPPでIPアドレスを取得します。PPPのカプセル化処理が入りますのでMobileEthernet0.0より速度はおそくなります。事業者で異なりますが、lcp echo によるkeepaliveが動作しますので、回線の異常監視ができます。アダプタモードでは、配下ルータでPPPoEクライアントを使用します。

●MobileEthernet0.0の動作概要

ネットワークアダプタ方式(NDIS接続)を使用して網と接続します。DHCPでIPアドレスを取得します。仮想LANのイメージとなり、PPPの様にカプセル化せずにEthernetのフレームで通信するため、高速化に対応します。LTEでの接続通信に有効です。

なお、データ通信端末によって、使用できるインタフェースは異なります。各データ通信端末で使用できるインタフェースについては＜付録＞をご参照ください。

以下にWA1510を例にSerial0とMobileEthernet0.0のデータ通信接続に関わる設定を対比して説明します。

ユーザID、パスワードの設定

データ通信端末が網接続するための認証情報の設定を行います。

● Serial0 の場合

グローバルコンフィグモードでppp profileを作成し、profile内でユーザID、パスワードを設定します。ユーザID、パスワードが任意の場合でも設定が必要です。インタフェースSerial0にてprofileの指定を行います。

```
WA1500(config)# ppp profile test [Enter]
WA1500(config-ppp[test])# authentication username test [Enter]
WA1500(config-ppp[test])# authentication password plain test [Enter]
WA1500(config-ppp[test])# exit [Enter]
WA1500(config)#
```

```
WA1500(config)# interface Serial0 [Enter]
WA1500(config-Serial0)# ppp profile test [Enter]
WA1500(config-Serial0)# exit [Enter]
WA1500(config)#
```

● MobileEthernet0.0の場合

認証設定が必須な場合、MobileEthernet0.0内でユーザID、パスワードの設定を行います。ユーザID、パスワードが任意の場合は、設定不要です。

```
WA1500# configure [Enter]
WA1500(config)# interface MobileEthernet0.0 [Enter]
WA1500(config-MobileEthernet0.0)# mobile username test [Enter]
WA1500(config-MobileEthernet0.0)# mobile password plain test [Enter]
WA1500(config-MobileEthernet0.0)#
```

接続先の設定

データ通信端末が利用する契約サービスの接続先を設定します。

- Serial0の場合

CID、DPD-Type、APNの指定をmobile id コマンドで設定を行います。
また、mobile number コマンドで、ダイヤルアップ番号の設定を行います。

```
WA1500(config)# interface Serial0 [Enter]
WA1500(config-Serial0)# mobile id ppp 1 net.example.com [Enter]
WA1500(config-Serial0)# mobile number *99***CID# [Enter]
WA1500(config-Serial0)# exit [Enter]
WA1500(config)#
```

- MobileEthernet0.0の場合

APNの指定をmobile id コマンドで設定を行います。
ダイヤルアップ番号の設定は不要です。

```
WA1500# configure [Enter]
WA1500(config)# interface MobileEthernet0.0 [Enter]
WA1500(config-MobileEthernet0.0)# mobile id ip net.example.com [Enter]
WA1500(config-MobileEthernet0.0)#
```

IPアドレスの設定

インタフェースが利用するIPアドレスの設定をします。

- Serial0の場合

PPPでは、ipcpでの取得となるため、ipcp指定の設定を行います。

```
WA1500# configure [Enter]
WA1500(config)# interface Serial0 [Enter]
WA1500(config-Serial0)# ip address ipcp [Enter]
WA1500(config-Serial0)#
```

メモ　WA1020では、アダプタモード動作のため、工場出荷時から、上記設定となっています。

- MobileEthernet0.0の場合

NDIS接続では、DHCPでの取得となるため、DHCPクライアント設定を行います。

```
WA1500# configure [Enter]
WA1500(config)# interface MobileEthernet0.0 [Enter]
WA1500(config-MobileEthernet0.0)# ip address dhcp [Enter]
WA1500(config-MobileEthernet0.0)#
```

接続動作の設定

網への接続を自動接続か、オンデマンド接続かの設定をします。

自動接続の場合、auto-connect を設定します。
オンデマンド接続の場合、no auto-connect を設定し、無通信タイマをidle-time コマンドで設定します。

Serial0とMobileEthernet0.0とで、設定に違いはありません。以下のオンデマンド接続設定は、無通信タイマを180秒[3分]で、送信方向のパケット通過を監視する設定の例です。

- Serial0の場合

自動接続設定

```
WA1500# configure [Enter]
WA1500(config)# interface Serial0 [Enter]
WA1500(config-Serial0)# auto-connect [Enter]
WA1500(config-Serial0)#
```

オンデマンド接続設定

```
WA1500# configure [Enter]
WA1500(config)# interface Serial0 [Enter]
WA1500(config-Serial0)# no auto-connect [Enter]
WA1500(config-Serial0)# idle time timer 180 [Enter]
WA1500(config-Serial0)#
```

- MobileEthernet0.0の場合

自動接続設定

```
WA1500# configure [Enter]
WA1500(config)# interface MobileEthernet0.0 [Enter]
WA1500(config-MobileEthernet0.0)# auto-connect [Enter]
WA1500(config-MobileEthernet0.0)#
```

オンデマンド接続設定

```
WA1500# configure [Enter]
WA1500(config)# interface MobileEthernet0.0 [Enter]
WA1500(config-MobileEthernet0.0)# no auto-connect [Enter]
WA1500(config-MobileEthernet0.0)# idle time timer 180 [Enter]
WA1500(config-MobileEthernet0.0)#
```

PINコードの設定　(任意)

PINコードによる認証機能を使用する場合に設定します。手順を説明します。

※例ではPINコード初期値を 「0000」、変更後のPINコードを 「1234」 としています。

① インタフェースのshutdown

② pin-authenticationコマンドによる認証の有効変更

③ PINコードの変更

④ mobile pinコマンドによるPIN登録とshutdown解除

⑤ コンフィグ保存、再起動

⑥ show mobile statusによる確認

①インタフェースのshutdown

使用するインタフェースをshutdownします。

- Serial0の場合

```
WA1500(config)# interface Serial0 [Enter]
WA1500(config-Serial0)# shutdown [Enter]
WA1500(config-Serial0)# exit [Enter]
WA1500(config)# exit [Enter]
WA1500#
```

- MobileEthernet0.0の場合

```
WA1500(config)# interface MobileEthernet0.0 [Enter]
WA1500(config-MobileEthernet0.0)# shutdown [Enter]
WA1500(config-MobileEthernet0.0)# exit [Enter]
WA1500(config)# exit [Enter]
WA1500#
```

②pin- authenticationコマンドによる認証の有効設定

特権モードにて pin-authenticationコマンドで、PINコード認証を有効化します。

```
WA1500# pin-authentication on 0000 [Enter]
WA1500#
```

③PINコードの変更

pin-code コマンドによりPINコードの変更を行います。

```
WA1500# pin-code 0000 1234 [Enter]
WA1500#
```

④mobile pin コマンドによるPIN登録とshutdown解除

インタフェースコンフィグレーションモードで、mobile pin コマンドによりPINコード登録を行います。Serial0とMobileEthernet0.0との設定は排他になっています。

- Serial0の場合

```
WA1500# configure [Enter]
WA1500(config)# interface Serial0 [Enter]
WA1500(config-Serial0)# mobile pin plain 1234 [Enter]
WA1500(config-Serial0)# no shutdown [Enter]
WA1500(config-Serial0)# exit [Enter]
WA1500(config)#
```

- MobileEthernet0.0の場合

```
WA1500# configure [Enter]
WA1500(config)# interface MobileEthernet0.0 [Enter]
WA1500(config-MobileEthernet0.0)# mobile pin plain 1234 [Enter]
WA1500(config-MobileEthernet0.0)# no shutdown [Enter]
WA1500(config-MobileEthernet0.0)# exit [Enter]
WA1500(config)#
```

<u>⑤コンフィグ保存、再起動</u>

PIN認証は、「PINコード待ち」状態となるため、設定を保存して再起動します。再起動時にmobile pinコマンドによる認証がスタートします。

```
WA1500(config)# save [Enter]
WA1500(config)# reboot [Enter]
Are you sure you want to reboot the router? (Yes or No): yes
# reboot....
```

<u>⑥show mobile statusによる確認</u>

show mobile statusコマンドにて、PIN認証が成功していることを確認します。

pin auth がdoneになり、pin auth failが0であることを確認します。

```
WA1500(config)# show mobile status [Enter]

                （略）

 pin status                : +CPIN: READY
 pin auth                  : done
 pin auth fail              : 0        ←―――――― 左記を確認

                （略）

WA1500(config)#
```

注意　PIN認証に失敗した状態で、PINコードの変更はできません。
通信端末のPINコードと、本装置に設定されたPINコードを一致させ、一度、PIN認証を成功させた後、上記手順をやり直してください。

注意　連続して3回PIN認証に失敗すると、PINロック状態（データ通信端末が使用できない状態）となります。
本製品では起動時に1回PIN認証を行いますので、間違ったPIN登録がされている場合、3回起動した時点かリカバリ機能によるUSB給電OFF/ONを3回実行した時点でPINロック状態となります。

注意　データ通信端末の仕様によっては、間違ったPINコードでの有効/無効、PINコード変更を繰り返した場合にPINロック状態となる場合があります。

メモ　PINロック状態を解除するためには、PINロック解除コード(PUKコード)が必要となります。本製品では、データ通信端末のPINロック解除を行うことはできませんので、データ通信端末のご購入元から提示される方法によりPINロック解除を実施してください。

メモ　WA1511の内蔵モジュールにて、PIN認証に失敗して、ロック状態になった場合は、ロック状態の解除にPINロック解除コードが必要となります。以下をご参照願います。解除コードは、SIMカードの契約先へお問い合わせください。

WA1511内蔵モジュールのPINロック解除手順

以下の手順でロックを解除してください。

(例:誤PINコード:7777、新PINコード:1234、PINロック解除コード:12345678)

① インタフェース MobileEthernet0.0のshutdown

② mobile pinコマンドの削除

③ PINロック解除コマンドでロック解除、新PINコード登録

④ 新しいPINコードでのmobile pinコマンド設定

⑤ インタフェース MobileEthernet0.0のshutdown解除

⑥ コンフィグ保存、再起動

①インタフェース MobileEthernet0.0のshutdown

MobileEthernet0.0をshutdownします。

```
WA1500(config)# interface MobileEthernet0.0 [Enter]
WA1500(config-MobileEthernet0.0)# shutdown [Enter]
WA1500(config-MobileEthernet0.0)# exit [Enter]
WA1500(config)#
```

②mobile pinコマンドの削除

PIN認証再設定のために、現在の誤ったPIN設定を削除します。

```
WA1500(config)# interface MobileEthernet0.0 [Enter]
WA1500(config-MobileEthernet0.0)# no mobile pin plain 7777 [Enter]
WA1500(config-MobileEthernet0.0)# exit [Enter]
WA1500(config)#
```

③PINロック解除コマンドでPINロック解除、新PINコード登録

内蔵モジュールのPINロック状態を解除し、同時に新しいPINコードを入力します。

```
WA1500(config)# pin-unlock 12345678 1234 [Enter]
WA1500(config)#
```

注意　PINロック解除コードは、事前にSIMカードの契約先へお問い合わせの上、入手をお願いします。

④新しいPINコードでmobile pinコマンドの設定

新しいPINコードを設定します。

```
WA1500(config)# interface MobileEthernet0.0 [Enter]
WA1500(config-MobileEthernet0.0)# mobile pin plain 1234[Enter]
WA1500(config-MobileEthernet0.0)# exit [Enter]
WA1500(config)#
```

⑤インタフェース MobileEthernet0.0のshutdown解除

MobileEthernet0.0をno shutdownします。

```
WA1500(config)# interface MobileEthernet0.0 [Enter]
WA1500(config-MobileEthernet0.0)# no shutdown [Enter]
WA1500(config-MobileEthernet0.0)# exit [Enter]
WA1500(config)#
```

⑥コンフィグ保存、再起動

PIN認証は、内蔵モジュールが「PINコード待ち」状態となるため、設定を保存して再起動します。

```
WA1500(config)# save [Enter]
WA1500(config)# reboot [Enter]
Are you sure you want to reboot the router? (Yes or No): yes
# reboot....
```

データ通信端末のリカバリ設定（任意）

データ通信端末が異常状態になり、自己復旧できない場合のリカバリ動作を設定します。Serial0 と MobileEthernet0.0 とで、設定に違いはありません。

- Serial0の場合

```
WA1500(config)# interface Serial0 [Enter]
WA1500(config-Serial0)# mobile zero-antenna-recovery enable [Enter]
WA1500(config-Serial0)# mobile auto-recovery enable [Enter]
WA1500(config-Serial0)# exit [Enter]
WA1500(config)#
```

メモ　WA1020は、mobile auto-recovery enable を工場出荷時に設定済みです。なお、コンフィグでは表示されません。

- MobileEthernet0.0の場合

```
WA1500(config)# interface MobileEthernet0.0 [Enter]
WA1500(config-MobileEthernet0.0)# mobile zero-antenna-recovery enable
[Enter]
WA1500(config-MobileEthernet0.0)# mobile auto-recovery enable [Enter]
WA1500(config-MobileEthernet0.0)# exit [Enter]
WA1500(config)#
```

■データ通信端末の設定について

以下のデータ通信端末を利用する場合は、ダイヤル発信時のATコマンドの設定が必要な場合があります。

C01LC、C02LC、203HW・・・mobile dial tone

以下のデータ通信端末を利用する場合は、LCP Echo-Request送信を無効にする必要があります。

DATA01、DATA03、DATA04、DATA07・・・no lcp echo enable

メモ　アダプタモードの場合は、WA1020への設定は不要です。

■データ通信端末の複数接続について

ソフトウェアバージョン4.0からデュアルキャリアに対応し、HSPA / LTE / PHSと、WiMAXデータ通信端末の同時利用が可能となりましたが、HSPA / LTE / PHSデータ通信端末同士、または、WiMAXデータ通信端末同士での同時利用はできませんのでご注意ねがいます。
WA1511は、USBポートにデータ通信端末または、WiMAXデータ通信端末を接続して、内蔵モジュールとの同時利用はできませんのでご注意ねがいます。

■データ通信端末の通信について

定額制契約のデータ通信端末にて定額制契約以外の設定により接続を行なった場合、従量課金による接続など予期せぬ通信費用が発生する場合がありますのでご注意ください。

従量制契約のデータ通信端末にて、長時間利用されますと予想外の通信費用が掛かる場合がありますのでご注意ください。

CIFS等のファイル共有を行う通信を行っている際に、実際に通信を行っていなくても定期的な通信が発生する場合があるため、意図しないダイヤルアップ接続が行われます。

このような場合は、意図しない不要なダイヤルアップ接続を抑えるフィルタ設定等をご検討下さい。

ご使用にあたっては設定の再確認や、定期的に通信量や通信費用をご確認いただくなどご注意いただくようお願いいたします。

無線データ通信は一般的にベストエフォート型の通信ですので、実際の通信速度が論理速度を下回る可能性があります。

また、本製品内にはルータ・アダプタ機能の処理があるため、データ通信端末をパソコンに直接続して使用する場合と比べ、通信速度が遅くなる可能性があります。

■無線LANを利用したデータ通信について

WA2021は無線LANカード「WA100-AP」を使用することで、無線LANアクセスポイントとして動作します。無線LAN規格IEEE802.11に準拠しておりますが、伝送速度300Mbps（IEEE802.11n規格値）、54Mbps（IEEE802.11g規格値）、11Mbps（IEEE802.11b規格値）は、無線LAN規格の理論上の最大値であり、実際のデータ伝送速度を示すものではありません。

無線LANの伝送速度や伝送距離は、周囲の環境条件（通信距離、障害物、電子レンジ等の電波環境要素、使用するパソコンの性能、ネットワークの使用状況など）により大きく変動します。

IEEE802.11b、IEEE802.11g、IEEE802.11nを使用する機器が混在している場合は、IEEE802.11nを使用する機器のスループットが著しく下がることがあります。

IEEE802.11n通信を行うためには、無線LAN端末の暗号化を「なし」、「WPA-PSK(AES)」または「WPA2-PSK(AES)」（推奨）に設定する必要があります。

また、複数のアクセスポイントが乱立する環境下では、スループットが低下したり、データが途切れたりする場合はあります。隣り合う無線チャネルのご利用は避けてください。

WiMAXデータ通信端末について

■WiMAX データ通信端末のファームウェアについて

本製品ではWiMAXデータ通信端末（※1）のイメージファイルを保持致します。

本製品のプログラムファイルをバージョンアップする事で、連動してWiMAXデータ通信端末のファームウェアもバージョンアップされますので、WiMAXデータ通信端末を本製品に装着したまま、WiMAXデータ通信端末のバージョンアップが行えると言ったメリットがございます。

しかしながらその反面、機能変更等によりWiMAXデータ通信端末のファームウェアに大幅な変更が生じた際には、本製品のバージョンアップが必要となる場合がございますので、ご了承下さい。

※1　2012年7月時点でのWiMAXデータ通信端末サポート機種は以下となります。

- AtermWM3200U ・・・ NEC アクセステクニカブランド(生産終了品)
- UD03NA ・・・ UQ コミュニケーションズブランド
- UD01NA ・・・ UQ コミュニケーションズブランド

■アダプタモードでの WiMAX 網から取得する DHCP 情報について

WiMAX網から通知されるDHCP情報は、一般的なDHCPサーバから通知される情報とは異なっているため、アダプタモードでは、WiMAX網から通知されるDHCP情報を以下のように変換を行います。変換されたDHCP情報を配下ルータに通知します。

サブネットマスク　：WiMAX 網から通知される値から 24 ビットに変換

例)（通知されるIPアドレス）192.168.10.1/32
（変換後のIPアドレス）　192.168.10.1/24

デフォルトゲートウェイ：WiMAX 網から通知される IP アドレスに 「+1」したアドレスに変換

例)（通知されるIPアドレス）192.168.10.100
（変換後のIPアドレス）　192.168.10.101
※ただし、「254」が通知された場合は「1」に変換します

また、WiMAX回線の接続、切断等によるIPアドレス変化に迅速に追従できる様に、リースタイム値を設定変更出来るようにしています。デフォルトは、60秒に変換します。

リースタイム　：WiMAX 網から通知される値をコンフィグ設定値に変換

■WiMAX データ通信端末を使用できる機器

WiMAXデータ通信端末を使用できる機器は、WA1020、WA2020、WA2021となります。

WA1510、WA1511はサポートしておりませんので、ご注意ねがいます。

4-2

初期設定の方法

最初に行う基本的な設定

本製品をご購入後、初めて行う最低限の設定について説明します。
本章は、CLIを使用した場合の説明をしています。Web-GUIをご利用の場合は、Web-GUIマニュアルをご参照ください。

設定は、次に示す基本的な設定をローカルコンソールで行います。

1) 接続の確認
2) 電源投入
3) アドミニストレータ権限のユーザ名／パスワード変更
4) 日付、時刻の設定
5) ホスト名の設定
6) リモートコンソールの設定
7) ランニングコンフィグの保存
8) コマンドによる再起動とログイン

1）接続の確認

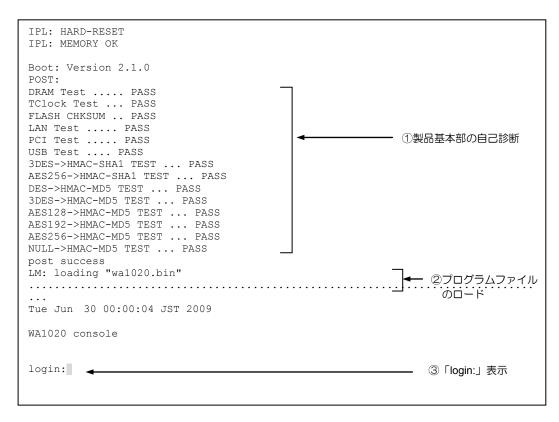
コンソールポートにケーブルが正しく接続されているか、データ通信端末、ACアダプタ、（WA1511の場合、SIMカード、アンテナ含む）が正しく接続されているか確認します。

2）電源投入

ACアダプタの電源プラグをACコンセントに接続します。システム状態が以下の順序で表示されます。

① 自己診断が実行されます。正常に終了すると、診断結果が「PASS」表示となります。

② プログラムファイルをロードします。ロードされるプログラムファイル名が表示されます。
プログラムファイルのロード中は、「....」で経過を表示します。

③ ロードが正常に終了すると、「login：」が表示されます。

メモ　機種ごとに表示内容が異なります。４章「基本操作と各種説明」に、起動時の表示内容を記載しています。

電源 OFF による終了

電源をOFFする際は、STATランプが点滅していないことを確認してから、ACアダプタの電源プラグをコンセントから抜いて終了します。

注意　製品本体とACアダプタ間のDCジャックの挿抜による電源の切断は行わないでください。

3) アドミニストレータ権限のユーザ名／パスワード変更

工場出荷時に設定されているアドミニストレータ権限のユーザ名／パスワードを変更します。

新規にアドミニストレータ権限のユーザ名／パスワードを設定します。ソフトウェアバージョン5.1.3までは、工場出荷時に設定されているアドミニストレータ権限のユーザへの上書き登録はできません。新規ユーザ追加後、出荷時設定のユーザを削除ねがいます。

グローバルコンフィグモードにおいてusernameコマンドにて新たなアドミニストレータ権限の設定を行った後、no usernameコマンドで工場出荷設定のユーザ名を削除します。no usernameのパラメータは、設定されているユーザ名（admin）です。usernameコマンドのパラメータは、ユーザ名、パスワード、ユーザ権限（administrator）です。ユーザ名は最大16文字までです。パスワードは最大128文字までです。

確認は、show running-configコマンドで行います。

メモ　パスワードの設定を平文（plain）で入力した後にshow running-configコマンドで設定を確認すると、パスワードはハッシュ値で表示されます。

注意　パスワードは決して忘れないように注意してください。特にすべてのアドミニストレータ権限ユーザのパスワードを忘れてしまった場合には、設定変更ができなくなります。この場合には、初期化をする必要があります。初期化では、ランニングコンフィグ、スタートアップコンフィグの設定情報が失われます。

なお、アドミニストレータ権限のユーザは、全て削除が出来ません。1ユーザは残ります。

セキュリティのため、パスワードは文字と数字を組み合わせるなど、推測しにくい組み合わせにしてください。

設定

例は、工場出荷時に設定されているアドミニストレータ権限の削除、新たなアドミニストレータ権限ユーザとしてユーザ名「WA1020-admin」、パスワード「abcd123」を登録しています。

```
WA1020(config)# username WA1020-admin password plain abcd123
administrator [Enter]
% User 'WA1020-admin' has been added. [Enter]              } 追加
WA1020(config)# no username admin [Enter]
% User 'admin' has been deleted.                           } 削除
WA1020(config)#
```

確認

確認は、show running-configコマンドで行います。

メモ　ユーザ名とユーザ権限が表示され、パスワードはハッシュ表示となります。

```
WA1020(config)# show running-config [Enter]
（途中省略）

username WA1020-admin password hash 6CE21C6C548272C27C administrator

（途中省略）
WA1020(config)#
```

4）日付、時刻の設定

WA1020は、カレンダー時計を内蔵していますが、電源バックアップ機能は有していません。したがって現在の日付、時刻を設定できますが、電源OFF/ONすると初期化されます。その場合の初期値は「2009年1月1日」となります。

WA1510、WA1511、WA2020、WA2021は、電源バックアップ機能付きのカレンダー時計を内蔵しています。したがって日付、時刻の設定をすれば、電源OFF/ONしても日付、時刻は保存されます。

WA1510、WA1511は、電源OFFしてから設定が保存されているのは約5日間で、それ以後は初期化され、初期値は「2014年1月1日」となります。

WA2020、WA2021は、電源OFFしてから設定が保存されているのは約10日間で、それ以後は初期化され、初期値は「2011年1月1日」となります。

時刻の設定は、clockコマンドで行います。clockコマンドのパラメータとしては、時(0-23)、分（0-59）、秒（0-59）、日（1-31）、月（1-12）、西暦年（2009-2037）の順序で、各パラメータ間にスペースを入れて入力します。確認は、show clockコマンドで行います。

注意　日付、時刻は特権モードでのみ設定ができます。

設定

例は、特権モードに移り、日本時刻として「2009年6月30日 午後4時12分0秒」を設定しています。時報や正確な時計などに合わせてclockコマンドを投入します。

```
WA1020# clock 16 12 0 30 6 2009 [Enter]
WA1020#
```

メモ　時刻のみを変更するときは、日、月、西暦年を省略して、時、分、秒のみの入力が可能です。

確認

```
WA1020(config)# show clock [Enter]
Tue 30 June 2009 16:12:03
uptime is 0 days 3 hours 13 minutes 31 secs.
WA1020(config)#
```

5). ホスト名の設定

本製品を識別するためにホスト名を設定します。ホスト名の設定は、グローバルコンフィグモードにおいてhostnameコマンドで行います。

設定と確認

例は、グローバルコンフィグモードに移り、ホスト名として「WA1020-01」を登録しています。コマンドプロンプトがホスト名で表示されることを確認します。

```
WA1020(config)# hostname WA1020-01 [Enter]
WA1020-01(config)#
```

6). リモートコンソールの設定

本製品をリモートコンソールで使用するための設定を行います。
WA1020で使用するアダプタモードでの設定およびルータモードでの設定をtelnet使用する場合、SSHを使用する場合で説明します。

■ルータモードの場合

- **telnet サーバ使用の場合**

①telnet サーバ起動の設定

telnetサーバの起動は、グローバルコンフィグモードの状態で、 telnet-server enableコマンドを使用して行います。

注意　リモートコンソールから本製品への不正なアクセスを防止するため、telnetサーバの起動はユーザアカウントの登録を行ってから実行してください。
ユーザアカウントの登録方法は、この章の「最初に行う基本的な設定 3.アドミニストレータ権限のユーザ名／パスワード変更」を参照してください。

```
WA1020-01(config)# telnet-server enable [Enter]
WA1020-01(config)#
```

②telnet サーバ設定の確認

確認は、show running-configコマンドで行います。

```
WA1020-01(config)# show running-config [Enter]

（途中省略）

telnet-server enable

WA1020-01(config)#
```

● SSH サーバ使用の場合

①SSH サーバ起動の設定

SSHサーバの起動は、グローバルコンフィグモードの状態で、 ssh-server enableコマンドを使用して行います。

注意　本コマンドで、SSHサーバを起動しても、秘密鍵、公開鍵を生成しなければSSHでの接続はできません。また、ユーザアカウントの登録を推奨します。ユーザアカウントの登録方法は、この章の「最初に行う基本的な設定 3.アドミニストレータ権限のユーザ名／パスワード変更」を参照してください。

```
WA1020-01(config)# ssh-server enable [Enter]
WA1020-01(config)#
```

②SSH サーバ秘密鍵/公開鍵の生成

SSHサーバの起動は、グローバルコンフィグモードの状態で、 ssh-server host-key generate rsaコマンドを使用して行います。

注意　鍵の確認は、showコマンドを使用しますが、秘密鍵は確認できません。

```
WA1020-01(config)# ssh-server host-key generate rsa [Enter]
Generating public/private rsa key pair..done
WA1020-01(config)#
```

③SSH サーバ設定の確認

設定の確認は、show running-configコマンドで行います。

```
WA1020-01(config)# show running-config [Enter]

（途中省略）

ssh-server enable          ←  「enable」になっていることを確認します。

WA1020-01(config)#
```

④SSH サーバ公開鍵の確認

公開鍵の確認は、show ssh-server host-key fingerprint コマンドで行います。

```
WA1020(config)# show ssh-server host-key fingerprint  [Enter]
RSA(2048) fingerprint:                      ← 「公開鍵」表示を確認します。
  MD5 b5:a4:b9:69:2e:d4:93:37:69:60:3e:1b:dc:72:bc:ea

WA1020(config)#
```

注意　SSHクライアントからの最初のssh接続時に公開鍵を確認する画面が表示されますので、コマンド表示の鍵と同じであることを確認します。

注意　装置を初期化すると、秘密鍵/公開鍵も削除されますので、鍵の再生成が必要です。

メモ　秘密鍵/公開鍵の生成/削除時は、自動的にフラッシュメモリに保存されるので、saveコマンドは不要です。また、コンフィグでは表示されません。

■アダプタモード(PPP接続)の場合

アダプタモードでリモートコンソールを使用する場合、ルータと本製品を接続しているインタフェース（ルータ側）にて、PPPoE用のサブインタフェースとEthernet用のインタフェース設定が必要となります。

(インターネットへは、配下ルータの PPPoE インタフェースから WA1020 を経由して通信します)

- **telnet サーバ使用の場合**

①スタティックルートの設定

ルータ配下の端末から通信を可能とするために、スタティックルートを設定します。

```
WA1020(config-FastEthernet0.0)# exit[Enter]
WA1020(config)# ip route default 192.168.1.254 [Enter]
WA1020(config)#
```

②telnet サーバ起動の設定

telnetサーバの起動は、グローバルコンフィグモードの状態で、 telnet-server enableコマンドを使用して行います。

注意　リモートコンソールから本製品への不正なアクセスを防止するため、telnetサーバの起動はユーザアカウントの登録を行ってから実行してください。
ユーザアカウントの登録方法は、この章の「最初に行う基本的な設定 3.アドミニストレータ権限のユーザ名／パスワード変更」を参照してください。

```
WA1020-01(config)# telnet-server enable [Enter]
WA1020-01(config)#
```

③telnet サーバ設定の確認

確認は、show running-configコマンドで行います。

```
WA1020-01(config)# show running-config [Enter]

（途中省略）

telnet-server enable

WA1020-01(config)#
```

④ルータの設定（UNIVERGE IXルータを使用した場合）

UNIVERGE IXルータの基本インタフェースであるFastEthernet1.0にIPアドレスを設定します。

例では、IPアドレスに192.168.1.254、サブネットマスク長24（255.255.255.0）を設定しています。

```
IX_Router(config)# interface FastEthernet1.0 [Enter]
IX_Router(config-FastEthernet1.0)# ip address 192.168.1.254/24 [Enter]
IX_Router(config-FastEthernet1.0)# no shutdown [Enter]
```

- **SSH サーバ使用の場合**

①スタティックルートの設定

ルータ配下の端末から通信を可能とするために、スタティックルートを設定します。

```
WA1020(config-FastEthernet0.0)# exit[Enter]
WA1020(config)# ip route default 192.168.1.254 [Enter]
WA1020(config)#
```

②SSH サーバ起動の設定

SSHサーバの起動は、グローバルコンフィグモードの状態で、 ssh-server enableコマンドを使用して行います。

注意　本コマンドで、SSHサーバを起動しても、秘密鍵、公開鍵を生成しなければSSHでの接続はできません。また、ユーザアカウントの登録を推奨します。ユーザアカウントの登録方法は、この章の「最初に行う基本的な設定 3.アドミニストレータ権限のユーザ名／パスワード変更」を参照してください。

```
WA1020-01(config)# ssh-server enable [Enter]
WA1020-01(config)#
```

③SSH サーバ秘密鍵/公開鍵の生成

SSHサーバの起動は、グローバルコンフィグモードの状態で、 ssh-server host-key generate rsaコマンドを使用して行います。

注意　鍵の確認は、showコマンドを使用しますが、秘密鍵は確認できません。

```
WA1020-01(config)# ssh-server host-key generate rsa [Enter]
Generating public/private rsa key pair..done
WA1020-01(config)#
```

④SSH サーバ設定の確認

設定の確認は、show running-configコマンドで行います。

```
WA1020-01(config)# show running-config [Enter]

（途中省略）

ssh-server enable          ←  「enable」になっていることを
                               確認します。

WA1020-01(config)#
```

⑤SSH サーバ公開鍵の確認

公開鍵の確認は、show ssh-server host-key fingerprint コマンドで行います。

```
WA1020(config)# show ssh-server host-key fingerprint  [Enter]
RSA(2048) fingerprint:                      ← 「公開鍵」表示を確認
  MD5 b5:a4:b9:69:2e:d4:93:37:69:60:3e:1b:dc:72:bc:ea   します。

WA1020(config)#
```

注意　SSHクライアントからの最初のssh接続時に公開鍵を確認する画面が表示されますので、コマンド表示の鍵と同じであることを確認します。

注意　装置を初期化すると、秘密鍵/公開鍵も削除されますので、鍵の再生成が必要です。

メモ　秘密鍵/公開鍵の生成/削除時は、自動的にフラッシュメモリに保存されるので、saveコマンドは不要です。また、コンフィグでは表示されません。

⑥ルータの設定（UNIVERGE IXルータを使用した場合）

UNIVERGE IXルータの基本インタフェースであるFastEthernet1.0にIPアドレスを設定します。

例では、IPアドレスに192.168.1.254、サブネットマスク長24（255.255.255.0）を設定しています。

```
IX_Router(config)# interface FastEthernet1.0 [Enter]
IX_Router(config-FastEthernet1.0)# ip address 192.168.1.254/24 [Enter]
IX_Router(config-FastEthernet1.0)# no shutdown [Enter]
```

■アダプタモード(WiMAX接続、NDIS接続)の場合

リモートコンソールを使用する場合、ルータと本製品を接続しているインタフェース（ルータ側）にて、DHCPクライアント用のインタフェース設定とUNIVERGE WA1020接続用のセカンダリIPアドレス設定が必要となります。1つのインタフェース上で上記機能が同時に動作するルータが必要となります。

(インターネットへは、配下ルータのDHCPクライアントで取得したIPアドレスでWA1020を通して通信します)

- **telnet サーバ使用の場合**

①スタティックルートの設定

ルータ配下の端末から通信を可能とするために、スタティックルートを設定します。

例では、デフォルトルートをルータのセカンダリIPアドレスを指定しています。

```
WA1020(config-FastEthernet0.0)# exit[Enter]
WA1020(config)# ip route default 192.168.1.254 [Enter]
WA1020(config)#
```

②telnet サーバ起動の設定

telnetサーバの起動は、グローバルコンフィグモードの状態で、 telnet-server enableコマンドを使用して行います。

注意　リモートコンソールから本製品への不正なアクセスを防止するため、telnetサーバの起動はユーザアカウントの登録を行ってから実行してください。
ユーザアカウントの登録方法は、この章の「最初に行う基本的な設定 3.アドミニストレータ権限のユーザ名／パスワード変更」を参照してください。

```
WA1020-01(config)# telnet-server enable [Enter]
WA1020-01(config)#
```

③telnet サーバ設定の確認

確認は、show running-configコマンドで行います。

```
WA1020-01(config)# show running-config [Enter]

（途中省略）

telnet-server enable

WA1020-01(config)#
```

④ルータの設定（UNIVERGE IXルータを使用した場合）

UNIVERGE WA1020との通信用のセカンダリIPアドレスを設定します。

例では、IPアドレスに192.168.1.254、サブネットマスク長24（255.255.255.0）を設定しています。

```
IX_Router(config)# interface FastEthernet1.0 [Enter]
IX_Router(config-FastEthernet1.0)# ip address 192.168.1.254/24 secondary
[Enter]
IX_Router(config-FastEthernet1.0)#
```

ただし、ルータにてnapt設定をしている場合は、UNIVERGE WA1020からの通信を透過させるため、napt処理を行わない設定を以下のように追加します。

```
IX_Router(config)# ip access-list jyogai deny ip src 192.168.1.0/24 dest
192.168.1.0/24 [Enter]
IX_Router(config)# ip access-list jyogai deny ip src 192.168.2.0/24 dest
192.168.1.0/24 [Enter]
IX_Router(config)# ip access-list jyogai permit ip src 192.168.2.0/24 dest
any [Enter]
IX_Router(config)# interface FastEthernet1.0 [Enter]
IX_Router(config-FastEthernet1.0)# ip napt inside list jyogai [Enter]
IX_Router(config-FastEthernet1.0)#
```

メモ　192.168.2.0/24は、リモートコンソールを使用する端末のLANアドレスです。

- **SSHサーバ使用の場合**

①スタティックルートの設定

ルータ配下の端末から通信を可能とするために、スタティックルートを設定します。

例では、デフォルトルートをルータのセカンダリIPアドレスを指定しています。

```
WA1020(config-FastEthernet0.0)# exit[Enter]
WA1020(config)# ip route default 192.168.1.254 [Enter]
WA1020(config)#
```

②SSH サーバ起動の設定

SSHサーバの起動は、グローバルコンフィグモードの状態で、 ssh-server enableコマンドを使用して行います。

注意　本コマンドで、SSHサーバを起動しても、秘密鍵、公開鍵を生成しなければSSHでの接続はできません。また、ユーザアカウントの登録を推奨します。ユーザアカウントの登録方法は、この章の「最初に行う基本的な設定 3.アドミニストレータ権限のユーザ名／パスワード変更」を参照してください。

```
WA1020-01(config)# ssh-server enable [Enter]
WA1020-01(config)#
```

③SSH サーバ秘密鍵/公開鍵の生成

SSHサーバの起動は、グローバルコンフィグモードの状態で、 ssh-server host-key generate rsaコマンドを使用して行います。

注意　鍵の確認は、showコマンドを使用しますが、秘密鍵は確認できません。

```
WA1020-01(config)# ssh-server host-key generate rsa [Enter]
Generating public/private rsa key pair..done
WA1020-01(config)#
```

④SSH サーバ設定の確認

設定の確認は、show running-configコマンドで行います。

```
WA1020-01(config)# show running-config [Enter]

（途中省略）

ssh-server enable        ←  「enable」になっていることを
                             確認します。

WA1020-01(config)#
```

⑤SSH サーバ公開鍵の確認

公開鍵の確認は、show ssh-server host-key fingerprint コマンドで行います。

```
WA1020(config)# show ssh-server host-key fingerprint  [Enter]
RSA(2048) fingerprint:                       ← 「公開鍵」表示を確認
  MD5 b5:a4:b9:69:2e:d4:93:37:69:60:3e:1b:dc:72:bc:ea   します。

WA1020(config)#
```

注意　SSHクライアントからの最初のssh接続時に公開鍵を確認する画面が表示されますので、コマンド表示の鍵と同じであることを確認します。

注意　装置を初期化すると、秘密鍵/公開鍵も削除されますので、鍵の再生成が必要です。

メモ　秘密鍵/公開鍵の生成/削除時は、自動的にフラッシュメモリに保存されるので、saveコマンドは不要です。また、コンフィグでは表示されません。

⑥ルータの設定（UNIVERGE IXルータを使用した場合）

UNIVERGE WA1020との通信用のセカンダリIPアドレスを設定します。

例では、IPアドレスに192.168.1.254、サブネットマスク長24（255.255.255.0）を設定しています。

```
IX_Router(config)# interface FastEthernet1.0 [Enter]
IX_Router(config-FastEthernet1.0)# ip address 192.168.1.254/24 secondary
[Enter]
IX_Router(config-FastEthernet1.0)#
```

ただし、ルータにてnapt設定をしている場合は、UNIVERGE WA1020からの通信を透過させるため、napt処理を行わない設定を以下のように追加します。

```
IX_Router(config)# ip access-list jyogai deny ip src 192.168.1.0/24 dest
192.168.1.0/24 [Enter]
IX_Router(config)# ip access-list jyogai deny ip src 192.168.2.0/24 dest
192.168.1.0/24 [Enter]
IX_Router(config)# ip access-list jyogai permit ip src 192.168.2.0/24 dest
any [Enter]
IX_Router(config)# interface FastEthernet1.0 [Enter]
IX_Router(config-FastEthernet1.0)# ip napt inside list jyogai [Enter]
IX_Router(config-FastEthernet1.0)#
```

メモ　192.168.2.0/24は、リモートコンソールを使用する端末のLANアドレスです。

7）ランニングコンフィグの保存

設定変更したデータは、DRAMエリアのランニングコンフィグに書きこまれています。したがって、電源がOFFになると消失してしまいます。

電源がOFFになっても消失しないように、ランニングコンフィグの内容をスタートアップコンフィグとして、フラッシュメモリに保存します。

スタートアップコンフィグへの保存は、saveコマンドで行います。スタートアップコンフィグは現在のランニングコンフィグに変更されれます。

保存

saveコマンドを投入すると、STATランプが赤点滅し、フラッシュメモリに書き込み中であることを知らせます。書き込みが終わると、STATランプは緑点灯し、コマンドプロンプトが表示されます。

```
WA1020-01(config)# save [Enter]
WA1020-01(config)#
```

注意　STATランプ点滅中は、ACアダプタを抜かないでください。フラッシュメモリのデータを破壊することがあります。

8）コマンドによる再起動とログイン

設定したデータが確実に保存され､そのデータを伴って再起動できるか確認します。
再起動は特権モードにおいてrebootコマンドで行います。

コマンドによる再起動

特権モードに移ってから、rebootコマンドにより再起動します。
起動後、登録したユーザ名、パスワードでログインします。
例では、アドミニストレータ権限で登録したユーザ名「WA1020-admin」、パスワード「abcd123」でログインしています。

```
WA1020# reboot [Enter]
Are you sure you want to reboot the router? (Yes or No): yes
# reboot....

IPL: SOFT-RESET
IPL: MEMORY OK

Boot: Version 2.1.0
POST:
DRAM Test ..... PASS
TClock Test ... PASS
FLASH CHKSUM .. PASS
LAN Test ..... PASS
PCI Test ..... PASS
USB Test .... PASS
3DES->HMAC-SHA1 TEST ... PASS
AES256->HMAC-SHA1 TEST ... PASS
DES->HMAC-MD5 TEST ... PASS
3DES->HMAC-MD5 TEST ... PASS
AES128->HMAC-MD5 TEST ... PASS
AES192->HMAC-MD5 TEST ... PASS
AES256->HMAC-MD5 TEST ... PASS
NULL->HMAC-MD5 TEST ... PASS
post success
LM: loading "wa1020.bin"
.........................................................................
.........
Thu Jan  1 00:03:52 JST 2009

WA1020 console

login: WA1020-admin [Enter]
Password: abcd123 [Enter]       ←（パスワードは表示されません）
Copyright (c) NEC Platforms, Ltd. 2009-2014 All rights reserved.
Copyright (c) 1996-2004
   The NetBSD Foundation, Inc.  All rights reserved.
Copyright (c) 1982, 1986, 1989, 1991, 1993
   The Regents of the University of California.  All rights reserved.
Enter configuration commands, one per line. End with CNTL/Z.
WA1020>
```

FE0/GE0/GE1 ポートの設定

FE0/GE0/GE1ポートの設定は、使用する環境に合わせて設定します。
ここでは各ポートの１例を示して説明します。

■設定方法

通信モードの設定は、サブコンフィグモード（インタフェース）で行います。
なお、本製品の初期値は、通信速度、通信方向ともにオートネゴシエーションです。
また、WA2020、WA2021については、通信モード以外にメディアタイプの設定変更ができます。

通信速度の設定

以下の例では、WA1020でのFE0ポートの通信速度を100Mbps、通信方向を全二重に設定しています。

```
WA1020# configure [Enter]
WA1020(config)# interface FastEthernet0.0 [Enter]
WA1020(config-FastEthernet0.0)# speed-duplex 100full [Enter]
WA1020(config-FastEthernet0.0)#
```

また、以下の例はWA2021でGE0ポートの通信速度を1000Mbps、通信方向を全二重に設定しています。

```
WA2021# configure [Enter]
WA2021(config)# interface GigaEthernet0.0 [Enter]
WA2021(config-GigaEthernet0.0)# speed-duplex 1000full [Enter]
WA2021(config-GigaEthernet0.0)#
```

以下の例は、WA2021 の GE1 の LAN1～4 の内の LAN1 ポートの通信速度を 1000Mbps、通信方向を全二重に設定しています。

```
WA2021# configure [Enter]
WA2021(config)# interface GigaEthernet1.0 [Enter]
WA2021(config-GigaEthernet1.0)# speed-duplex 1000full port 1 [Enter]
WA2021(config-GigaEthernet1.0)#
```

注意　WA2020、WA2021 の GE1 ポートで設定する通信速度、通信方向は、ソフトウェアバージョン 4.1 以前ではポート単位での設定は出来ません。
ソフトウェアバージョン 4.2 以降ではポート単位の設定が可能です。

注意　本製品のFE0/GE0/GE1ポートに通信機器（HUB等）を接続した場合、本製品または対向する通信機器の片方がオートネゴシエーション設定のとき、リンクが確立しているにもかかわらず、両者通信モードの不一致により転送効率が悪くなることがあります。
このような場合、双方の機器にて100M 全二重もしくは1000M 全二重の固定設定を行います。

メディアタイプの設定

以下の例は、WA2021 の GE1 のメディアタイプを MDI に設定しています。

```
WA2021# configure [Enter]
WA2021(config)# interface GigaEthernet1.0 [Enter]
WA2021(config-GigaEthernet1.0)# l2sw-mdi mdi [Enter]
WA2021(config-GigaEthernet1.0)#
```

注意　WA1020、WA1510、WA1511 では、メディアタイプの Auto-MDI/MDIX を変更することはできません。

メモ　WA2020、WA2021 の GE1 ポートでは、メディアタイプの MDI/MDIX は 4 ポート共に同一の設定となります。

設定の確認

設定した内容をshow interfacesコマンドで確認します。

```
WA1020(config)# show interfaces FastEthernet0.0 [Enter]
Interface FastEthernet0.0 is up

（途中省略）

  Physical layer is up
  Physical address 00:02:00:00:00:01
  Media Ethernet autoselect ( 100baseTX full-duplex )

（途中省略）

WA1020(config)#
```

設定内容を確認します。
(例では 100Mbps、全二重)

GE1ポートで設定した内容を確認する場合は、show l2sw portsコマンドを使用します。

```
WA2021(config)# show l2sw ports
interface GigaEthernet1.0
  port 1: link UP autoselect ( 1000baseT full-duplex )
  port 2: link UP autoselect ( 100baseTX full-duplex )
  port 3: link DOWN autoselect ( 100baseTX full-duplex )
  port 4: link DOWN autoselect ( 100baseTX full-duplex )
WA2021(config)#
```

設定内容を確認します。
(例では全二重、100Mbps)

メモ　メディアタイプの設定内容は、show running-config で確認します。

5

ネットワーク設定例

アダプタモード設定例（PPPの場合）

アダプタモードにおける基本的な設定を説明します。本設定により、配下に接続するルータからインターネットアクセス等を行うことが可能となります。本モードはWA1020のみ有効です。
各コマンドの詳細については、コマンドリファレンスをご参照ください。

以下の手順にて設定を行います。

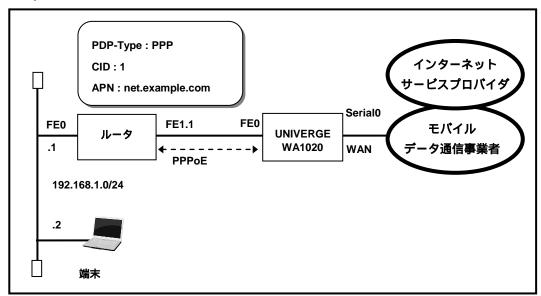
1） 配下ルータのPPP、PPPoE設定

※Service-Nameタグが設定可能なルータの場合、本製品（工場出荷状態の場合）はコンフィグレスで動作しますので以下の設定（2～4）は不要です。

2） アダプタモード設定の確認

3） アクセスポイントの設定

4） ダイヤルアップ番号の設定

5） 接続

メモ		
PDP-Type	：	パケット通信の通信方式を指定します。IPまたはPPPが指定可能です。
APN	：	アクセスポイントネーム。パケット通信の接続先を指定するパラメータです。 データ通信端末のSIMカード内に登録される情報で、購入時に初期値が設定されている場合があります。
CID	：	データ通信端末内に保存されているAPNを示す番号です。 データ通信端末のSIMカード内に登録される情報で、購入時に初期値が設定されている場合があります。
Number	：	APNに対応したダイヤルアップ番号です。

※PDP-Type、APN、CID、Number およびユーザID、パスワード情報は、モバイルデータ通信事業者にご確認ください。

注意　アダプタモードでお使いになる場合、本製品と配下ルータを接続する際に必ず両者を直に接続してください。両者の間にスイッチングHUBなどを介すると通信不能になる恐れがあります。

1） 配下ルータのPPP、PPPoE設定

本製品のアダプタモードを利用する場合、配下ルータにてPPPとPPPoEの設定を行います。

なお、Service-Name タグが設定可能なルータの場合、Service-Nameタグに、PDP-Type、CID、APN、Numberを設定することで、本製品を設定することなく（コンフィグレス）使用可能となります。

メモ　Service-Name ： ISP名やサービス名を指定することで、特定のサービスを選択可能となります。
※本製品では、PDP-Type、CID、APN、Numberの設定に使用されます。

以下は、UNIVERGE IXルータを使用した場合の設定例です。

```
IX_Router(config)# ppp profile test [Enter]
IX_Router(config-ppp-test)# authentication myname test [Enter]
IX_Router(config-ppp-test)# authentication password test test [Enter]
IX_Router(config-ppp-test)# exit [Enter]
IX_Router(config)# interface FastEthernet1.1 [Enter]
IX_Router(config-FastEthernet1.1)# encapsulation pppoe [Enter]
IX_Router(config-FastEthernet1.1)# auto-connect [Enter]
IX_Router(config-FastEthernet1.1)# pppoe service-name ppp,1,net.example.com [Enter]
IX_Router(config-FastEthernet1.1)# ppp binding test [Enter]
IX_Router(config-FastEthernet1.1)# ip address ipcp [Enter]
IX_Router(config-FastEthernet1.1)# no shutdown [Enter]
```

メモ　Service-Nameタグの設定は、カンマ区切りでPDP-Type、CID、APN、Number(ダイヤルアップ番号)の順で設定を行います。（Numberは省略可能です）

Numberの指定は、ダイヤルアップ番号の最後がCIDを用いないタイプの電話番号の際に必要となります。

注意　本製品をコンフィグレスで使用する場合、配下ルータのPPP認証はPAP認証のみとなります。CHAP認証を使用する場合は、本製品の設定が必要となります。

メモ　Service-Nameタグの設定ができないルータを使用される場合は、以降の手順にて本製品に対する設定を行います。

2） アダプタモード設定の確認

工場出荷時（初期値）はアダプタモードとなっています。

設定が異なっている場合は、wireless-adapter enable を設定してください。

```
WA1020(config)#  wireless-adapter enable [Enter]
WA1020(config)#
```

3） アクセスポイントの設定

Serial0のインタフェースコンフィグモードに移行します。

mobile id コマンドにて、PDP-Type、CID、APNの順で設定を行います。

```
WA1020(config)# interface Serial0 [Enter]
WA1020(config-Serial0)# mobile id PPP 1 net.example.com [Enter]
WA1020(config-Serial0)#
```

4） ダイヤルアップ番号の設定

ダイヤルアップ番号は、mobile number コマンドにて設定を行います。

```
WA1020(config-Serial0)# mobile number *99***CID# [Enter]
WA1020(config-Serial0)#
```

メモ　工場出荷時（初期値）は、上記ダイヤルアップ番号が設定されています。

5） 接続

配下ルータからのPPPoEパケットをトリガに接続を開始します。

注意　データ通信端末にて、従量制の契約を行なっている場合、長時間の接続で高額な費用が掛かる場合がありますのでご注意ください。

以下、上記で説明した2項から4項まで設定したWA1020の設定を示します。

```
hostname WA1020
!
wireless-adapter enable
!
interface FastEthernet0.0
  ip address 192.168.1.200/24
  no shutdown
!
interface Serial0
  ip address ipcp
  mobile id PPP 1 net.example.com
  mobile number *99***CID#
  auto-connect
  no shutdown
!
```

アダプタモード設定例（WiMAXの場合）

WiMAXでのアダプタモードにおける基本的な設定を説明します。本設定により、配下に接続しているルータからインターネットアクセス等を行うことが可能となります。本モードはWA1020のみ有効です。

各コマンドの詳細については、コマンドリファレンスをご参照ください。

以下の手順にて設定を行います。

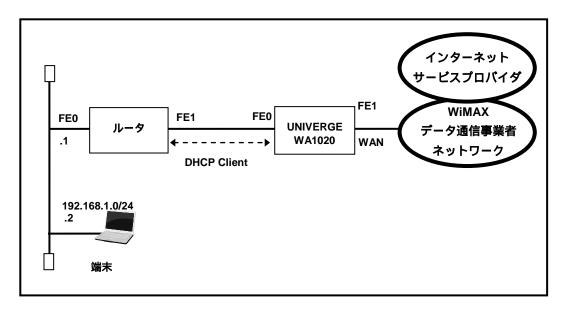
1） 配下ルータのDHCPクライアント設定

※本製品（工場出荷状態の場合）にWiMAXデータ通信端末を接続して、電源ONする事で、WiMAX利用のアダプタモードで起動します。コンフィグレスで動作しますので以下の設定（2～3）は不要です。

2） アダプタモード設定の確認

3） WiMAXインタフェース設定の確認

4） 配下ルータのNAPT設定

5） 接続

注意 ・電源ON時に、データ通信端末の通信方式を判断しますので、ご使用になるデータ通信端末を本製品に接続してから、電源ONにしてください。

・本製品では、サービス加入手続きが完了していないWiMAXデータ通信端末はご利用になれません

・アダプタモードでお使いになる場合、本製品と配下ルータを接続する際に必ず両者を直に接続してください。両者の間にスイッチングHUBなどを介すると通信不能になる恐れがあります。

・アダプタモードにて配下ルータに通知するデフォルトゲートウェイは、WiMAX網への接続のために本製品にて変換された値となります。
pingによる死活監視や疎通確認には利用しないでください。

・配下ルータの仕様により、WiMAX回線の再接続などで、DHCPで付与されるIPアドレスが変更された場合に、通信が復旧しないものがあります。その場合は、ルータ側での対応が必要になります。
（ルータの再起動やDHCPクライアント初期化等）

1） 配下ルータのDHCPクライアント設定

本製品のWiMAXでのアダプタモードを利用する場合、配下ルータにてDHCPクライアントの設定を行います。

なお、本製品を設定することなく（コンフィグレス）使用可能となります。

以下は、UNIVERGE IXルータを使用した場合の設定例です。

```
IX_Router(config)# interface FastEthernet1.0 [Enter]
IX_Router(config-FastEthernet1.0)# ip address dhcp receive-default [Enter]
IX_Router(config-FastEthernet1.0)# ip tcp adjust-mss auto [Enter]
IX_Router(config-FastEthernet1.0)# no shutdown [Enter]
```

メモ　DHCP サーバからのデフォルトゲートウェイ通知を受け入れます。

2） アダプタモード設定の確認

工場出荷時（初期値）はアダプタモードとなっています。

設定が異なっている場合は、wireless-adapter enable を設定してください。

```
WA1020(config)#  wireless-adapter enable [Enter]
WA1020(config)#
```

3） WiMAXインタフェース設定の確認

FastEthernet1.0のインタフェースがあることを確認します。

FastEthernet1.0のインタフェースが表示されない場合、WiMAXが動作するモードに移行していませんので、データ通信端末の接続を確認して、電源OFF／ONを実施願います。

```
WA1020(config)# interface FastEthernet1.0 [Enter]
WA1020(config-FastEthernet1.0)#
WA1020(config-FastEthernet1.0)#
```

存在しない場合は、以下の表示となります。

```
WA1020(config)# interface FastEthernet1.0 [Enter]
% FastEthernet1.0      -- Invalid command.
WA1020(config)#
```

４） 配下ルータのNAPT設定

配下ルータのインタフェースFastEthernet1.0にNAPT設定を行い、複数台の端末が同時にインターネット接続できるように設定します。

```
IX_Router(config)# interface FastEthernet1.0 [Enter]
IX_Router(config-FastEthernet1.0)# ip napt enable [Enter]
IX_Router(config-FastEthernet1.0)# exit [Enter]
IX_Router(config)#
```

５） 接続

データ通信端末による自動接続となる為、自動的に接続を開始します。

以下、上記2,3項で説明したWA1020の設定(出荷状態)を示します。

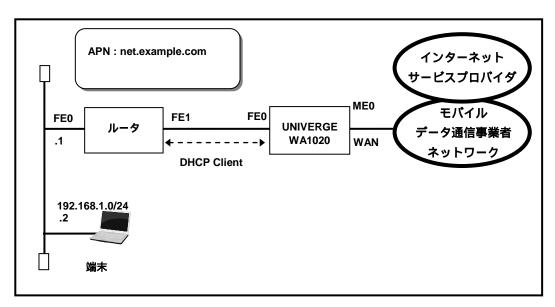
```
hostname WA1020
!
wireless-adapter enable
!
interface FastEthernet0.0
  ip address 192.168.1.200/24
  no shutdown
!
interface FastEthernet1.0
  no ip address
  auto-connect
  no shutdown
!
```

アダプタモード設定例（NDISの場合）

NDIS接続でのアダプタモードにおける基本的な設定を説明します。本設定により、配下に接続しているルータからインターネットアクセス等を行うことが可能となります。本モードはWA1020のみ有効です。

各コマンドの詳細については、コマンドリファレンスをご参照ください。

以下の手順にて設定を行います。

1） 配下ルータのDHCPクライアント設定
2） アダプタモード設定の確認
3） MobileEthernet0.0インタフェース設定の確認
4） 配下ルータのNAPT設定
5） 接続

メモ　APN　：　アクセスポイントネーム。パケット通信の接続先を指定するパラメータです。データ通信端末の SIM カード内に登録される情報で、購入時に初期値が設定されている場合があります。
APN、およびユーザ ID、パスワード情報は、モバイルデータ通信事業者にご確認ください。

注意　・電源ON時に、データ通信端末の通信方式を判断しますので、ご使用になるデータ通信端末を本製品に接続してから、電源ONにしてください。

・アダプタモードでお使いになる場合、本製品と配下ルータを接続する際に必ず両者を直に接続してください。両者の間にスイッチングHUBなどを介すると通信不能になる恐れがあります。

・pingによる死活監視や疎通確認には利用しないでください。

・配下ルータの仕様によっては、NDIS再接続などDHCPで付与されるIPアドレスが

変更された場合に、通信が復旧しないものがあります。その場合は、ルータ側での対応が必要になります。
（ルータの再起動やDHCPクライアント初期化等）

1） 配下ルータのDHCPクライアント設定

配下ルータにてDHCPクライアントの設定を行います。

以下は、UNIVERGE IXルータを使用した場合の設定例です。

```
IX_Router(config)# interface FastEthernet1.0 [Enter]
IX_Router(config-FastEthernet1.0)# ip address dhcp receive-default [Enter]
IX_Router(config-FastEthernet1.0)# ip tcp adjust-mss auto [Enter]
IX_Router(config-FastEthernet1.0)# no shutdown [Enter]
```

メモ　DHCP サーバからのデフォルトゲートウェイ通知を受け入れます。

2） アダプタモード設定の確認

工場出荷時（初期値）はSerial0/FastEthernet0.0アダプタモードとなっています。

アダプタモードをNDIS接続モード（MobileEthernet0.0）としてください。

```
WA1020(config)#  wireless-adapter enable MobileEthernet0.0[Enter]
WA1020(config)#
```

3） MobileEthernet0.0インタフェース設定の確認

MobileEthernet0.0のインタフェースコンフィグモードに移行します。

mobile id コマンドにてAPNの設定、さらに認証設定のユーザID、パスワードの設定後、インタフェースをUPします。

```
WA1020(config)# interface MobileEthernet0.0 [Enter]
WA1020(config-MobileEthernet0.0)# mobile id ip net.example.com [Enter]
WA1020(config-MobileEthernet0.0)# mobile username test@example.com [Enter]
WA1020(config-MobileEthernet0.0)# mobile password plain test [Enter]
WA1020(config-MobileEthernet0.0)# no shutdown
```

4） 配下ルータのNAPT設定

配下ルータのインタフェースFastEthernet1.0にNAPT設定を行い、複数台の端末が同時にインターネット接続できるように設定します。

```
IX_Router(config)# interface FastEthernet1.0 [Enter]
IX_Router(config-FastEthernet1.0)# ip napt enable [Enter]
IX_Router(config-FastEthernet1.0)# exit [Enter]
IX_Router(config)#
```

５） 接続

データ通信端末による自動接続となる為、自動的に接続を開始します。

以下、上記2,3項で説明したWA1020の設定を示します。

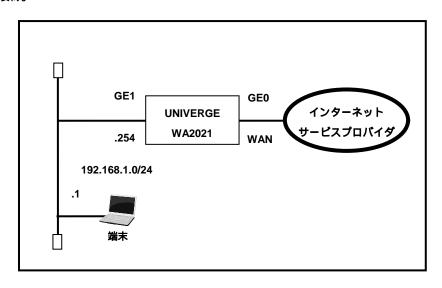
```
hostname WA1020
!
wireless-adapter enable MobileEthernet0.0
!
interface FastEthernet0.0
  ip address 192.168.1.200/24
  no shutdown
!
interface MobileEthernet1.0
  no ip address
  mobile id IP net.example.com
  mobile username test@example.com
  mobile password plain test
  auto-connect
  no shutdown
!
```

ルータモード設定例（PPPoEの場合）

ルータモードにおける基本的なPPPoE接続の設定を説明します。本設定により、本製品からインターネットアクセス等を行うことが可能となります。PPPoE接続は、WA1510、WA1511、WA2020とWA2021で有効です。

各コマンドの詳細については、コマンドリファレンスをご参照ください。

以下の手順にて設定を行います。

1） PPPプロファイル設定
2） PPPoEインタフェース設定
3） NAPT設定
4） 物理インタフェース（GE0）の設定
5） プロキシDNS設定
6） DHCPサーバ設定
7） LANインタフェース（GE1）設定
8） ルーティング設定
9） 接続

メモ　PPP に利用する、ユーザ ID／パスワード情報は、インターネットサービスプロバイダにご確認ください。

1） PPPプロファイルの設定

PPP関連の設定プロファイルを作成します。

```
WA2021(config)# ppp profile test [Enter]
WA2021(config-ppp[test])# authentication username test@example.com [Enter]
WA2021(config-ppp[test])# authentication password plain test [Enter]
WA2021(config-ppp[test])# exit [Enter]
```

2） PPPoEインタフェース設定

PPPoEインタフェースを作成し、PPPプロファイルを適用します。
IPアドレス設定はIPCPを設定します。
またTCPセッション確立時のMSS値の設定を行います。

```
WA2021(config)# interface PPPoE0 [Enter]
WA2021(config-PPPoE0)# ip address ipcp [Enter]
WA2021(config-PPPoE0)# ppp profile test [Enter]
WA2021(config-PPPoE0)# ip tcp adjust-mss auto [Enter]
WA2021(config-PPPoE0)# auto-connect [Enter]
WA2021(config-PPPoE0)# no shutdown [Enter]
```

メモ　PPPoE インタフェース作成時はデフォルトで、「auto-connect」が設定されます。

3） NAPT設定

インタフェースPPPoE0にNAPT設定を行い、複数台の端末が同時にインターネット接続できるように設定します。

```
WA2021(config-PPPoE0)# ip napt enable [Enter]
WA2021(config-PPPoE0)# exit [Enter]
WA2021(config)#
```

4） 物理インタフェース（GE0）の設定

PPPoEを利用する物理インタフェース（GigaEthernet0.0）に、PPPoEインタフェースを割り当てる設定を行います。

```
WA2021(config)# interface GigaEthernet0.0 [Enter]
WA2021(config-GigaEthernet0.0)# no ip address [Enter]
WA2021(config-GigaEthernet0.0)# encapsulation PPPoE0 [Enter]
WA2021(config-GigaEthernet0.0)# no shutdown [Enter]
WA2021(config-GigaEthernet0.0)# exit [Enter]
WA2021(config)#
```

注意　PPPoE インタフェースを割り当てる物理インタフェースは、「no shutdown」としておく必要があります。

5） プロキシDNS設定

プロキシDNSの設定を行います。DNSサーバ情報をIPCPにより自動取得する場合は以下のように設定します。

```
WA2021(config)# proxy-dns server default PPPoE0 ipcp [Enter]
WA2021(config)# proxy-dns enable [Enter]
```

6） DHCPサーバ設定

本製品のDHCPサーバ機能を使用して、LAN側のPC等にIPアドレスを割り当てる場合、以下のように設定します。

```
WA2021(config)# ip dhcp-server profile test [Enter]
WA2021(config-dhcps-profile[test])# assignable-range 192.168.1.1 10 [Enter]
WA2021(config-dhcps-profile[test])# default-gateway auto [Enter]
WA2021(config-dhcps-profile[test])# dns-server auto [Enter]
WA2021(config-dhcps-profile[test])# subnet-mask auto [Enter]
WA2021(config-dhcps-profile[test])# exit [Enter]
WA2021(config)# ip dhcp-server enable [Enter]
```

7） LANインタフェース（GE1）設定

LANインタフェースのIPアドレス設定を行い、DHCPサーバ機能をインタフェースに適用します。

```
WA2021(config)# interface GigaEthernet1.0 [Enter]
WA2021(config-GigaEthernet1.0)# ip address 192.168.1.254/24 [Enter]
WA2021(config-GigaEthernet1.0)# ip dhcp-server binding test [Enter]
WA2021(config-GigaEthernet1.0)# no shutdown [Enter]
WA2021(config-GigaEthernet1.0)# exit [Enter]
WA2021(config)#
```

8） ルーティング設定

インタフェースPPPoE0をデフォルトルートとして設定します。

```
WA2021(config)# ip route default PPPoE0 [Enter]
WA2021(config)#
```

9） 接続

PPPoEインタフェースの作成時は、自動接続（転送パケットの有無に関わらず常時接続、auto-connect設定）となっている為、自動的に接続を開始します。

no auto-connect コマンドにて要求時接続（PPPoEインタフェースへのパケット送信をトリガに接続開始）に変更することも可能です。

要求時接続の場合、idle-time timer コマンドで設定した無通信時間（初期値：600秒）を経過すると自動的に切断します。

```
WA2021(config-PPPoE0)# no auto-connect [Enter]
WA2021(config-PPPoE0)# idle-time timer 1800 [Enter]
```

注意　idle-time timer コマンド初期値を設定した場合は、コンフィグに表示されませんのでご注意ください。

以下、上記1項から8項で説明したPPPoEに関する設定を示します。

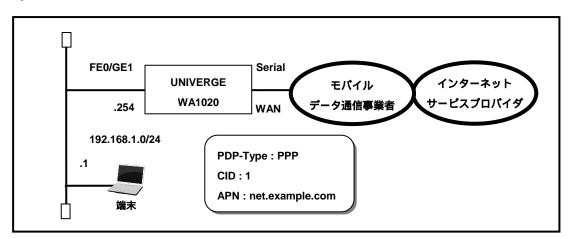
```
hostname WA2021
!
ppp profile test
  authentication username test@example.com
  authentication password plain test
!
!
ip dhcp-server enable
ip dhcp-server profile test
  assignable-range 192.168.1.1 10
  default-gateway auto
  dns-server auto
  subnet-mask auto
!
!
interface GigaEthernet0.0
  no ip address
  encapsulation PPPoE0
  no shutdown
!
interface GigaEthernet1.0
  ip address 192.168.1.254/24
  ip dhcp-server binding test
  no shutdown
!
interface PPPoE0
  ip address ipcp
  ip tcp adjust-mss auto
  ppp profile test
  auto-connect
  ip napt enable
  no shutdown
!
!
ip route default PPPoE0
!
proxy-dns enable
proxy-dns server default PPPoE0 ipcp
!
```

ルータモード設定例（PPPの場合）

PPP接続でのルータモードにおける基本的な設定を説明します。本設定により、端末からインターネットアクセスを行うことが可能となります。

各コマンドの詳細については、コマンドリファレンスをご参照ください。

以下の手順にて設定を行います。

1） ルータモード設定（WA1020のみ）
2） アクセスポイントの設定
3） ダイヤルアップ番号の設定
4） プロキシDNS設定
5） DHCPサーバ設定
6） LANインタフェース設定
7） NAPT設定
8） ルーティング設定
9） 接続

メモ

PDP-Type	：	パケット通信の通信方式を指定します。IPまたはPPPが指定可能です。
APN	：	アクセスポイントネーム。パケット通信の接続先を指定するパラメータです。 データ通信端末のSIMカード内に登録される情報で、購入時に初期値が設定されている場合があります。
CID	：	データ通信端末内に保存されているAPNを示す番号です。 データ通信端末のSIMカード内に登録される情報で、購入時に初期値が設定されている場合があります。
Number	：	APNに対応したダイヤルアップ番号です。

※PDP-Type、APN、CID、Number およびユーザID、パスワード情報は、モバイルデータ通信事業者にご確認ください。

注意　　WA1511は、Serial0での接続をサポートしておりません。

1）　ルータモード設定

工場出荷時（初期値）はアダプタモードとなっていますので、no wireless-adapter enable コマンドにてルータモードに変更します。(WA1020のみ)

```
WA1020(config)#  no wireless-adapter enable [Enter]
WA1020(config)#
```

2）　アクセスポイントの設定

PPP関連の設定プロファイルを作成後、Serial0インタフェースに適用します。
さらに mobile id コマンドにて、PDP-Type、CID、APNの順で設定を行います。

```
WA1020(config)# ppp profile test [Enter]
WA1020(config-ppp[test])# authentication username test [Enter]
WA1020(config-ppp[test])# authentication password plain test [Enter]
WA1020(config-ppp[test])# exit [Enter]
WA1020(config)# interface Serial0 [Enter]
WA1020(config-Serial0)# ppp profile test [Enter]
WA1020(config-Serial0)# mobile id ppp 1 net.example.com [Enter]
WA1020(config-Serial0)# ip address ipcp [Enter]
WA1020(config-Serial0)# no shutdown [Enter]
```

3）　ダイヤルアップ番号の設定

ダイヤルアップ番号は、mobile number コマンドにて設定を行います。

```
WA1020(config-Serial0)# mobile number *99***CID# [Enter]
WA1020(config-Serial0)# exit [Enter]
WA1020(config)#
```

メモ　　工場出荷時（初期値）は、上記ダイヤルアップ番号が設定されています。

4）　プロキシDNS設定

プロキシDNSの設定を行います。DNSサーバ情報をIPCPにより自動取得する場合は以下のように設定します。

```
WA1020(config)# proxy-dns server default Serial0 ipcp [Enter]
WA1020(config)# proxy-dns enable [Enter]
WA1020(config)#
```

5）　DHCPサーバ設定

本製品のDHCPサーバ機能を使用して、LAN側のPC等にIPアドレスを割り当てる場合、
以下のように設定します。

```
WA1020(config)# ip dhcp-server profile test [Enter]
WA1020(config-dhcps-profile[test])# assignable-range 192.168.1.1 10 [Enter]
WA1020(config-dhcps-profile[test])#default-gateway auto [Enter]
WA1020(config-dhcps-profile[test])#dns-server auto [Enter]
WA1020(config-dhcps-profile[test])#subnet-mask auto [Enter]
WA1020(config-dhcps-profile[test])#exit [Enter]
WA1020(config)# ip dhcp-server enable [Enter]
```

6） LANインタフェース設定

LANインタフェースのIPアドレス設定を行い、DHCPサーバ機能をインタフェースに適用します。

```
WA1020(config)# interface FastEthernet0.0 [Enter]
WA1020(config-FastEthernet0.0)# ip address 192.168.1.254/24 [Enter]
WA1020(config-FastEthernet0.0)# ip dhcp-server binding test [Enter]
WA1020(config-FastEthernet0.0)# exit [Enter]
WA1020(config)#
```

7） NAPT設定

インタフェースSerial0にNAPT設定を行い、複数台の端末が同時にインターネット接続できるように設定します。

```
WA1020(config)# interface Serial0 [Enter]
WA1020(config-Serial0)# ip napt enable [Enter]
WA1020(config-Serial0)# exit [Enter]
WA1020(config)#
```

8） ルーティング設定

インタフェースSerial0をデフォルトルートとして設定します。

```
WA1020(config)# ip route default Serial0 [Enter]
WA1020(config)#
```

9） 接続

工場出荷時（初期値）は、自動接続（転送パケットの有無に関わらず常時接続）となっている為、自動的に接続を開始します。

no auto-connect コマンドにて要求時接続（WAN側インタフェースへのパケット送信をトリガに接続開始）に変更することも可能です。
要求時接続の場合、idle-time timer コマンドで設定した無通信時間（初期値：600秒）を経過すると自動的に切断します。

```
WA1020(config-Serial0)# no auto-connect [Enter]
WA1020(config-Serial0)# idle-time timer 1800 [Enter]
```

注意　データ通信端末にて、従量制の契約を行なっている場合、長時間の接続で高額な費用が掛かる場合がありますのでご注意ください。

注意　上記では、初期値で、idle-time timer コマンドを入力しておりますが、初期値はコンフィグに表示されませんのでご注意ください。

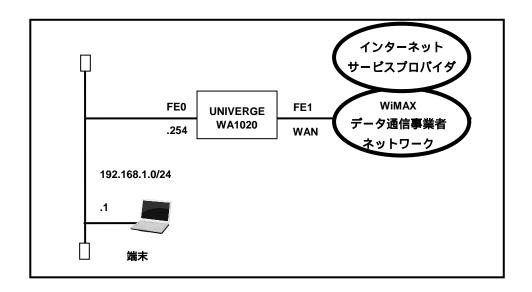
以下、上記1項から9項で説明した設定を示します。

```
hostname WA1020
!
!
no wireless-adapter enable
!
ppp profile test
  authentication username test
  authentication password plain test
!
!
ip dhcp-server enable
ip dhcp-server profile test
  assignable-range 192.168.1.1 10
  default-gateway auto
  dns-server auto
  subnet-mask auto
!
!
interface FastEthernet0.0
  ip address 192.168.1.254/24
  ip dhcp-server binding test
  no shutdown
!
interface Serial0
  ip address ipcp
  ppp profile test
  mobile id ppp 1 net.example.com
  mobile number *99***CID#
  ip napt enable
  auto-connect
  no shutdown
!
!
ip route default Serial0
!
proxy-dns enable
proxy-dns server default Serial0 ipcp
!
!
```

ルータモード設定例（WiMAXの場合）

WiMAX接続でのルータモードにおける基本的な設定を説明します。本設定により、端末からインターネットアクセスを行うことが可能となります。
各コマンドの詳細については、コマンドリファレンスをご参照ください。

以下の手順にて設定を行います。

1） ルータモード設定(WA1020のみ)
2） WiMAXインタフェースの設定
3） プロキシDNS設定
4） DHCPサーバ設定
5） LANインタフェース設定
6） NAPT設定
7） ルーティング設定
8） 接続

注意 ・本製品での認証登録は実施できません。認証を得ていない端末では、エラーとなり、通信できません。

・電源ON時に、データ通信端末の通信方式を判断しますので、ご使用になるデータ通信端末を本製品に接続してから、電源ONにしてください。

・WiMAX網から通知される デフォルトゲートウェイは、ネクストホップに存在しませんので、pingによる死活監視や疎通確認に使用することは適切ではありません。
※接続する通信事業者（MVNO事業者）によって、応答が返って来ない場合があります。

・WA1510、WA1511は、WiMAXデータ通信端末をサポートしておりません。

1） ルータモード設定

工場出荷時（初期値）はアダプタモードとなっていますので、no wireless-adapter enable コマンドにてルータモードに変更します。（WA1020のみ）

```
WA1020(config)#  no wireless-adapter enable [Enter]
WA1020(config)#
```

2） WiMAXインタフェースの設定

WiMAX用接続インタフェースのFastEthernet1.0を設定します。

網からIPアドレス等を取得するために、DHCPクライアントの設定を行います。

またTCPセッション確立時のMSS値の設定を行います。

FastEthernet1.0のインタフェースが表示されない場合、WiMAXが動作するモードに移行していませんので、データ通信端末の接続を確認して、電源OFF／ONを実施願います。

```
WA1020(config)# interface FastEthernet1.0 [Enter]
WA1020(config-FastEthernet1.0)# ip address dhcp [Enter]
WA1020(config-FastEthernet1.0)# ip tcp adjust-mss auto [Enter]
WA1020(config-FastEthernet1.0)# no shutdown [Enter]
WA1020(config-FastEthernet1.0)# exit [Enter]
WA1020(config)#
```

FastEthernet1.0が存在しない場合は、以下の表示となります。

```
WA1020(config)# interface FastEthernet1.0 [Enter]
% FastEthernet1.0      -- Invalid command.
WA1020(config)#
```

3）プロキシDNS設定

プロキシDNSの設定を行います。DNSサーバ情報をDHCPより自動取得する場合は以下のように設定します。

```
WA1020(config)# proxy-dns server default FastEthernet1.0 dhcp [Enter]
WA1020(config)# proxy-dns enable [Enter]
WA1020(config)#
```

4） DHCPサーバ設定

本製品のDHCPサーバ機能を使用して、LAN側のPC等にIPアドレスを割り当てる場合、以下のように設定します。

```
WA1020(config)# ip dhcp-server profile test [Enter]
WA1020(config-dhcps-profile[test])# assignable-range 192.168.1.1 10 [Enter]
WA1020(config-dhcps-profile[test])#default-gateway auto [Enter]
WA1020(config-dhcps-profile[test])#dns-server auto [Enter]
WA1020(config-dhcps-profile[test])#subnet-mask auto [Enter]
WA1020(config-dhcps-profile[test])#exit [Enter]
WA1020(config)# ip dhcp-server enable [Enter]
```

5） LANインタフェース設定

LANインタフェースのIPアドレス設定を行い、DHCPサーバ機能をインタフェースに適用します。

```
WA1020(config)# interface FastEthernet0.0 [Enter]
WA1020(config-FastEthernet0.0)# ip address 192.168.1.254/24 [Enter]
WA1020(config-FastEthernet0.0)# ip dhcp-server binding test [Enter]
WA1020(config-FastEthernet0.0)# exit [Enter]
WA1020(config)#
```

6） NAPT設定

インタフェースFastEthernet1.0にNAPT設定を行い、複数台の端末が同時にインターネット接続できるように設定します。

```
WA1020(config)# interface FastEthernet1.0 [Enter]
WA1020(config-FastEthernet1.0)# ip napt enable [Enter]
WA1020(config-FastEthernet1.0)# exit [Enter]
WA1020(config)#
```

7） ルーティング設定

インタフェース FastEthenet1.0をデフォルトルートとして設定します。

```
WA1020(config)# ip route default FastEthernet1.0 [Enter]
WA1020(config)#
```

8） 接続

データ通信端末による自動接続となる為、自動的に接続を開始します。

以下、上記1項から7項で説明した設定を示します。

```
hostname WA1020
!
!
no wireless-adapter enable
!
!
ip dhcp-server enable
ip dhcp-server profile test
  assignable-range 192.168.1.1 10
  default-gateway auto
  dns-server auto
  subnet-mask auto
!
!
interface FastEthernet0.0
  ip address 192.168.1.254/24
  ip dhcp-server binding test
  no shutdown
!
interface FastEthernet1.0
```

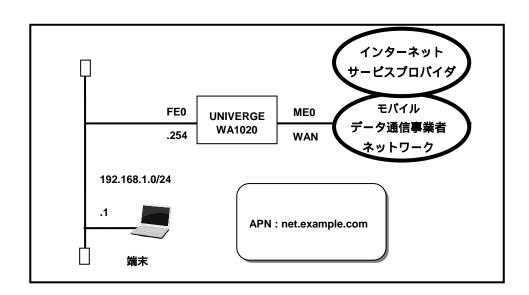
```
  ip address dhcp
  ip tcp adjust-mss auto
  auto-connect
  ip napt enable
  no shutdown
!
!
ip route default FastEthernet1.0
!
proxy-dns enable
proxy-dns server default FastEthernet1.0 dhcp
!
```

ルータモード設定例（NDISの場合）

NDIS接続でのルータモードにおける基本的な設定を説明します。本設定により、端末からインターネットアクセスを行うことが可能となります。

各コマンドの詳細については、コマンドリファレンスをご参照ください。

以下の手順にて設定を行います。

1） ルータモード設定(WA1020のみ)
2） MobileEthernet0.0インタフェースの設定
3） プロキシDNS設定
4） DHCPサーバ設定
5） LANインタフェース設定
6） NAPT設定
7） ルーティング設定
8） 接続

メモ　APN　：アクセスポイントネーム。パケット通信の接続先を指定するパラメータです。
データ通信端末の SIM カード内に登録される情報で、購入時に初期値が設定されている場合があります。

※APN、およびユーザID、パスワード情報は、モバイルデータ通信事業者にご確認ください。

1） ルータモード設定

工場出荷時（初期値）はアダプタモードとなっていますので、no wireless-adapter enable コマンドにてルータモードに変更します。（WA1020のみ）

```
WA1020(config)#  no wireless-adapter enable [Enter]
WA1020(config)#
```

2） MobileEthernet0.0インタフェースの設定

NDIS接続用インタフェースのMobileEthernet0.0を設定します。
mobile id コマンドにて、APNの設定を行います。
認証設定のユーザID、パスワードの設定を行います。
さらに網からIPアドレス等を取得するために、DHCPクライアントの設定を行います。
またTCPセッション確立時のMSS値の設定を行います。
設定後、インタフェースをUPします。

```
WA1020(config)# interface MobileEther0.0 [Enter]
WA1020(config-MobileEthernet0.0)# mobile id ip net.example.com [Enter]
WA1020(config-MobileEthernet0.0)# mobile username test@example.com [Enter]
WA1020(config-MobileEthernet0.0)# mobile password plain test [Enter]
WA1020(config-MobileEthernet0.0)# ip address dhcp [Enter]
WA1020(config-MobileEthernet0.0)# ip tcp adjust-mss auto [Enter]
WA1020(config-MobileEthernet0.0)# no shutdown [Enter]
```

メモ　MobileEthernet0.0インタフェースをUPした場合、Serial0インタフェースは自動的にDOWNします。また、Serial0インタフェースをUPした場合、MobileEthernet0.0インタフェースは自動的にDOWNします。

3）プロキシDNS設定

プロキシDNSの設定を行います。DNSサーバ情報をDHCPより自動取得する場合は以下のように設定します。

```
WA1020(config)# proxy-dns server default MobileEthernet0.0 dhcp [Enter]
WA1020(config)# proxy-dns enable [Enter]
WA1020(config)#
```

4） DHCPサーバ設定

本製品のDHCPサーバ機能を使用して、LAN側のPC等にIPアドレスを割り当てる場合、以下のように設定します。

```
WA1020(config)# ip dhcp-server profile test [Enter]
WA1020(config-dhcps-profile[test])# assignable-range 192.168.1.1 10 [Enter]
WA1020(config-dhcps-profile[test])#default-gateway auto [Enter]
WA1020(config-dhcps-profile[test])#dns-server auto [Enter]
WA1020(config-dhcps-profile[test])#subnet-mask auto [Enter]
WA1020(config-dhcps-profile[test])#exit [Enter]
WA1020(config)# ip dhcp-server enable [Enter]
```

５） LANインタフェース設定

LANインタフェースのIPアドレス設定を行い、DHCPサーバ機能をインタフェースに適用します。

```
WA1020(config)# interface FastEthernet0.0 [Enter]
WA1020(config-FastEthernet0.0)# ip address 192.168.1.254/24 [Enter]
WA1020(config-FastEthernet0.0)# ip dhcp-server binding test [Enter]
WA1020(config-FastEthernet0.0)# exit [Enter]
WA1020(config)#
```

６） NAPT設定

インタフェースFastEthernet1.0にNAPT設定を行い、複数台の端末が同時にインターネット接続できるように設定します。

```
WA1020(config)# interface MobileEthernet0.0 [Enter]
WA1020(config-MobileEthernet0.0)# ip napt enable [Enter]
WA1020(config-MobileEthernet0.0)# exit [Enter]
WA1020(config)#
```

７） ルーティング設定

インタフェース MobileEthenet0.0をデフォルトルートとして設定します。

```
WA1020(config)# ip route default MobileEthernet0.0 [Enter]
WA1020(config)#
```

８） 接続

データ通信端末による自動接続となる為、自動的に接続を開始します。

以下、上記1項から7項で説明した設定を示します。

```
hostname WA1020
!
!
no wireless-adapter enable
!
!
ip dhcp-server enable
ip dhcp-server profile test
  assignable-range 192.168.1.1 10
  default-gateway auto
  dns-server auto
  subnet-mask auto
!
!
interface FastEthernet0.0
  ip address 192.168.1.254/24
  ip dhcp-server binding test
  no shutdown
!
interface MobileEthernet0.0
```

```
  ip address dhcp
  mobile id IP net.example.com
  mobile username test@example.com
  mobile password plain test
  ip tcp adjust-mss auto
  auto-connect
  ip napt enable
  no shutdown
!
!
ip route default MobileEthernet0.0
!
proxy-dns enable
proxy-dns server default MobileEthernet0.0 dhcp
!
```

VLAN設定例

タグVLANを使用した設定を説明します。本設定によりLANインタフェースに複数のIPセグメントの接続が可能となり、セグメント間のルーティングが可能となります。

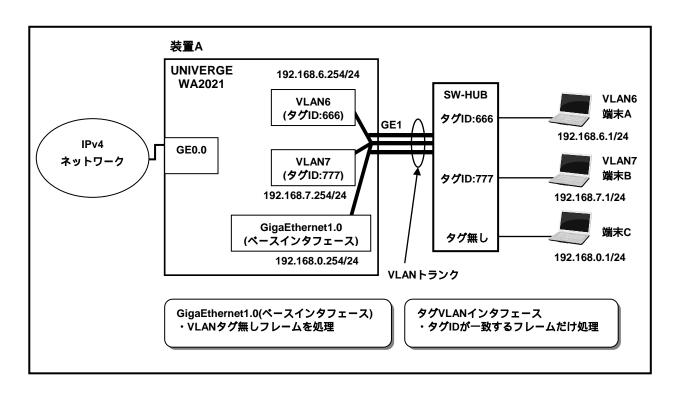
以下では、WA2021のGigaEthernet1.0インタフェースにタグVLANを設定する例を示します。

各コマンドの詳細については、コマンドリファレンスをご参照ください。ルータのWAN側の設定やデフォルトルートの通信設定は、完了している状態からの説明とします。

以下の手順にて設定を行います。

1）VLANインタフェースの設定

2）ベースインタフェースの設定

3）タグVLANの設定

ここでは、タグ付き VLAN フレームとタグ無しの非 VLAN フレームの両方の処理を行うハイブリッド動作の VLAN の設定を示します。

・タグVLANのインタフェースとして、VLAN6インタフェースとVLAN7インタフェースを使用します。GE1ポートに流れるタグ付きパケットのうち、指定されたタグのパケットのみを転送するためのインタフェースです。

・ベースインタフェースであるGigaEthernet1.0は、タグ無しの非VLANフレーム用として使用します。GE1に流れるタグ無しのパケットを転送します。

・VLANインタフェースのVLANtypeとタグIDの割り当てをベースインタフェースに設定することで、各VLANインタフェースの動作を指定します。

1） VLANインタフェースの設定

タグVLANのインタフェースとして用いるVLAN6インタフェースとVLAN7インタフェースを作成し、それぞれにルーティングするためのIPアドレスを設定します。

l VLAN6インタフェースの作成

```
WA2021(config)# interface vlan6 [Enter]
WA2021(config-vlan6)# ip address 192.168.6.254/24 [Enter]
WA2021(config-vlan6)# exit [Enter]
WA2021(config)#
```

l VLAN7インタフェースの作成

```
WA2021(config)# interface vlan7 [Enter]
WA2021(config-vlan7)# ip address 192.168.7.254/24 [Enter]
WA2021(config-vlan7)# exit [Enter]
WA2021(config)#
```

2）ベースインタフェースの設定

ベースインタフェースであるGigaEthernet1.0に、タグ無しの非VLANフレームをルーティングするためのIPアドレスを設定します。

```
WA2021(config)# interface GigaEthernet1.0 [Enter]
WA2021(config-GigaEthernet1.0)# ip address 192.168.0.254/24 [Enter]
WA2021(config-GigaEthernet1.0)#
```

3）タグVLANの設定

VLANインタフェースのVLANtypeとタグIDの割り当てをベースインタフェースに設定します。VLAN6インタフェースをタグID:666のタグVLANインタフェースとして、VLAN7インタフェースをタグID:777のタグVLANインタフェースとして設定します。

```
WA2021(config-GigaEthernet1.0)#
WA2021(config-GigaEthernet1.0)# vlan-type tagged VLAN6 tag-id 666 [Enter]
WA2021(config-GigaEthernet1.0)# vlan-type tagged VLAN7 tag-id 777 [Enter]
WA2021(config-GigaEthernet1.0)# exit [Enter]
WA2021(config)#
```

メモ　ベースインタフェースは、タグ無しの非VLANフレームのみ処理します。VLANタグが付いたフレームは、タグIDが一致するVLANインタフェースで処理します。

メモ　LAN１～LAN4 ポート間で、ブロードキャストドメインを分離したい場合は、タグVLAN のポート指定が可能です。ポート指定をした場合は、ベースインタフェースは使用できません。

注意　VLAN機能については、注意点および制限事項があります。詳細については、＜付録＞の「VLAN機能の注意点」をご参照ください。

以下、上記で説明したタグ VLAN の設定を示します。

装置 A

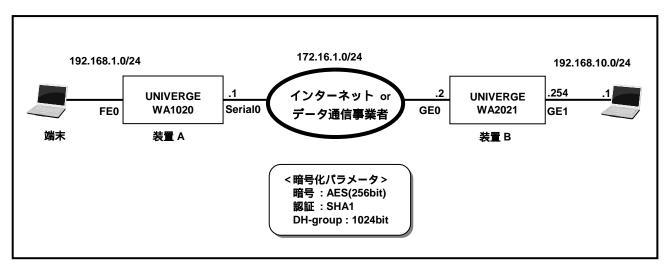
```
hostname WA2021
!
interface GigaEthernet1.0
  vlan-type tagged VLAN6 tag-id 666
  vlan-type tagged VLAN7 tag-id 777
  ip address 192.168.0.254/24
  no shutdown
!
interface VLAN6
  ip address 192.168.6.254/24
  no shutdown
!
interface VLAN7
  ip address 192.168.7.254/24
  no shutdown
!
```

IPsecメインモード設定例

IPsecのメインモードにおける基本的な設定を説明します。本設定により、メインモードでのIPsec通信が可能となります。PPPoE回線とHSPA端末を利用したトンネルモードを使用した例です。

各コマンドの詳細については、コマンドリファレンスをご参照ください。ルータの基本的な通信設定は、完了している状態からの説明とします。

以下の手順にて設定を行います。

1） IKEプロポーザルの設定
2） IKEポリシーの設定
3） IPsecプロポーザルの設定
4） IPsecポリシーの設定
5） IPsecプロファイルの設定
6） IPsecインタフェースの設定
7） ルーティングの設定
8） フィルタの設定

ここでは、装置A（WA1020）にてHSPA端末を利用し、装置B（WA2021）にてPPPoE回線を利用した、メインモードの設定を示します。

・WAN側は、固定のIPアドレスが払い出されるものとして設定します。

・IPsecの設定は、物理回線やインタフェースに依存しないため、装置Aと装置Bとも同じポリシーで設定が可能です。

・本設定例は、peer設定、IPアドレス等を除き、装置A、装置Bともに共通の設定となります。

※設定に必要となる暗号キーやプロポーザル/ポリシー名等は、事前に決定しておくと設定がスムーズに進みます。

注意　WA1511は、Serial0をサポートしておりません。MobileEthernet0.0を使用してください。

1） IKEプロポーザルの設定

ike proposalコマンドにて、作成するIKEプロポーザル名を指定し、モードを移ります。

暗号化アルゴリズム、認証アルゴリズム、IKE SAの有効時間を設定します。プロポーザル内の各設定を省略した場合は、自動的に初期値が登録されます。

```
WA1020(config)# ike proposal ikeprop1 [Enter]
WA1020(config-ike-proposal[ikeporp1])# encryption-algorithm aes256-cbc
[Enter]
WA1020(config-ike-proposal[ikeporp1])# authentication-algorithm  hmac-sha1
[Enter]
WA1020(config-ike-proposal[ikeporp1])# lifetime 28800 [Enter]
WA1020(config-ike-proposal[ikeporp1])# dh-group 1024-bit [Enter]
WA1020(config-ike-proposal[ikeporp1])# exit [Enter]
WA1020(config)#
```

2） IKEポリシーの設定

ike policyコマンドにて、作成するIKEポリシー名を指定し、モードを移ります。

使用するプロポーザルの設定、動作モードの設定（main、aggressive）、事前共有鍵の設定、IDペイロードの設定を行います。IDを設定しない場合は、自動的にSerial0のIPアドレスがIDとして使用されます。

メインモードとして動作させるため、modeをmainとします。

```
WA1020(config)# ike policy ikepol1 [Enter]
WA1020(config-ike-policy[ikepol1])# mode main [Enter]
WA1020(config-ike-policy[ikepol1])# dpd-keepalive enable 20 3
WA1020(config-ike-policy[ikepol1])# proposal ikeprop1 [Enter]
WA1020(config-ike-policy[ikepol1])# pre-shared-key plain hogehoge [Enter]
WA1020(config-ike-policy[ikepol1])# exit[Enter]
```

3） IPsecプロポーザルの設定

ipsec proposalコマンドにて、作成するIPsecプロポーザル名を指定し、モードを移ります。

暗号化アルゴリズム、認証アルゴリズムを設定します。IPsec SAの有効時間を設定します。プロポーザル内の各設定を省略した場合は、自動的に初期値が登録されます。

メモ　IPsec の暗号化アルゴリズムと認証アルゴリズムは複数設定可能です。

```
WA1020(config)# ipsec proposal ipsecprop1 [Enter]
WA1020(config-ipsec-proposal[ipsecprop1)# protocol esp enc-algo aes256-cbc
auth-algo hmac-sha1-96 [Enter]
WA1020(config-ipsec-proposal[ipsecprop1)# lifetime 28800 [Enter]
WA1020(config-ipsec-proposal[ipsecprop1)# exit [Enter]
WA1020(config)#
```

4） IPsecポリシーの設定

ipsec policyコマンドにて、IPsecポリシー名を指定し、モードを移ります。

利用するIKEプロポーザル、IPsec SAの自動更新の有無、PFS機能、ESP のセキュリティレベルの設定等をおこないます。ポリシー内の各設定を省略した場合は、自動的に初期値が登録されます。

```
WA1020(config)# ipsec policy ipsecpol1 [Enter]
WA1020(config-ipsec-policy[ipsecpol1])# proposal ipsecprop1 [Enter]
WA1020(config-ipsec-policy[ipsecpol1])# rekey enable [Enter]
WA1020(config-ipsec-policy[ipsecpol1])# exit [Enter]
WA1020(config)#
```

メモ　IPsec SAの自動更新機能は、省略するとrekey enableが設定されます。通信がある間は、自動更新しますが、該当SAで通信が無い場合は、自動更新されません。

5） IPsecプロファイルの設定

ipsec profileコマンドにて、IPsecプロファイル名を指定し、モードを移ります。

利用するIPsecポリシー、利用するIKEポリシー、peer （対向先）、source （SAを確立するインタフェース）、modeを設定します。sourceは、省略可能です。modeはトンネルモードを指定します。

l 装置A（WA1020の場合）

```
WA1020(config)# ipsec profile ipsecprof1 [Enter]
WA1020(config-ipsec-profile[ipsecprof1])# ipsec policy ipsecpol1 [Enter]
WA1020(config-ipsec-profile[ipsecprof1])# ike policy ikepol1 [Enter]
WA1020(config-ipsec-profile[ipsecprof1])# peer 172.16.1.2 [Enter]
WA1020(config-ipsec-profile[ipsecprof1])# mode tunnel [Enter]
WA1020(config-ipsec-profile[ipsecprof1])# exit [Enter]
WA1020(config)#
```

l 装置B（WA2021の場合）

```
WA2021(config)# ipsec profile ipsecprof1 [Enter]
WA2021(config-ipsec-profile[ipsecprof1])# ipsec policy ipsecpol1 [Enter]
WA2021(config-ipsec-profile[ipsecprof1])# ike policy ikepol1 [Enter]
WA2021(config-ipsec-profile[ipsecprof1])# peer 172.16.1.1 [Enter]
WA2021(config-ipsec-profile[ipsecprof1])# mode tunnel [Enter]
WA2021(config-ipsec-profile[ipsecprof1])# exit [Enter]
WA2021(config)#
```

注意　メインモードでは、peerコマンドにてany指定はできません。対向先のIPアドレスを明示してください。

注意　sourceを省略した場合は、peerに対するルーティングに従い、出力インタフェースのIPアドレスが利用されます。出力インタフェースがオンデマンド設定（no auto-connect）の場合は、sourceを省略することは出来ません。

６） IPsec インタフェースの設定

本製品ではIPsec通信を行うために、専用のIPsecインタフェースを利用します。
IPsecインタフェースの設定を行うため、インタフェースコンフィグモードに移ります。
IPアドレスの設定、利用するIPsecプロファイルの設定、tcp-mss調整の設定を行います。

```
WA1020(config)# interface IPsec0 [Enter]
WA1020(config-IPsec0)# ip address unnumbered [Enter]
WA1020(config-IPsec0)# ipsec map ipsecprof1 [Enter]
WA1020(config-IPsec0)# ip tcp adjust-mss auto [Enter]
WA1020(config-IPsec0)# no shutdown [Enter]
WA1020(config-IPsec0)# exit [Enter]
WA1020(config)#
```

７） ルーティングの設定

IPsec通信を使用する通信をIPsecインタフェースに転送する設定をおこないます。

l 装置A（WA1020の場合）

```
WA1020(config)# ip route default IPsec0 [Enter]
WA1020(config)# ip route 172.16.1.2/32 Serial0 [Enter]
WA1020(config)#
```

l 装置B（WA2021の場合）

```
WA2021(config)# ip route default IPsec0 [Enter]
WA2021(config)# ip route 172.16.1.1/32 PPPoE0 [Enter]
WA2021(config)#
```

８） フィルタの設定

各装置の出力インタフェース（WA1020:Serial0、WA2021:PPPoE0）にフィルタの設定を行います。IPsecのESP(プロトコル番号：50)とIKE（UDP：500）を許可します。

l 装置A（WA1020の場合）

```
WA1020(config)# ip access-list list1 permit 50 src 172.16.1.2/32 dest
172.16.1.1/32
WA1020(config)# ip access-list list1 permit udp src 172.16.1.2/32 sport any
dest 172.16.1.1/32 dport eq 500
WA1020(config)# interface Serial0
WA1020(config-Serial0)# ip filter list1 1 in
```

l 装置B（WA2021の場合）

```
WA2021(config)# ip access-list list1 permit 50 src 172.16.1.1/32 dest
172.16.1.2/32
WA2021(config)# ip access-list list1 permit udp src 172.16.1.1/32 sport any
dest 172.16.1.2/32 dport eq 500
WA2021(config)# interface PPPoE0
WA2021(config-PPPoE0)# ip filter list1 1 in
```

注意　本例では、物理インタフェースでNAPTは行わず、フィルタ設定を行っております。NAPTを有効にした場合は、フィルタと同様のNAPT除外設定が必要になります。

以下、上記で説明した装置A、装置Bの設定についてIPsec設定を中心に示します。

装置 A

```
!
hostname WA1020
!
ip access-list list1 permit 50 src 172.16.1.2/32 dest 172.16.1.1/32
ip access-list list1 permit udp src 172.16.1.2/32 sport any dest 172.16.1.1/32 dport eq 500
!
no wireless-adapter enable
!
ppp profile test
  authentication username test
  authentication password plain test
!
!
interface FastEthernet0.0
  ip address 192.168.1.254/24
  no shutdown
!
interface Serial0
  ip address ipcp
  ppp profile test
  ip filter list1 1 in
  mobile id PPP 1 net.example.com
  mobile number *99***CID#
  auto-connect
  no shutdown
!
interface IPsec0
  ip address unnumbered
  ip tcp adjust-mss auto
  ipsec map ipsecprof1
  no shutdown
!
!
ip route 172.16.1.2/32 Serial0
ip route default IPsec0
!
!
ike proposal ikeprop1
  encryption-algorithm aes256-cbc
  authentication-algorithm hmac-sha1
  lifetime 28800
  dh-group 1024-bit
!
ike policy ikepol1
  mode main
  dpd-keepalive enable 20 3
  proposal ikeprop1
  pre-shared-key plain hogehoge
!
!
ipsec proposal ipsecprop1
  protocol esp enc-algo aes256-cbc auth-algo hmac-sha1-96
  lifetime 28800
!
ipsec policy ipsecpol1
  proposal ipsecprop1
!
ipsec profile ipsecprof1
  mode tunnel
  ipsec policy ipsecpol1
  ike policy ikepol1
  peer 172.16.1.2
!
```

装置 B

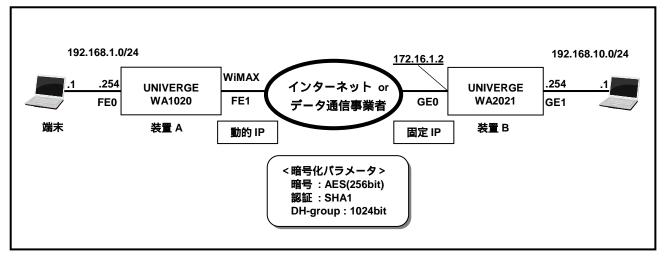
```
hostname WA2021
!
ip access-list list1 permit 50 src 172.16.1.1/32 dest 172.16.1.2/32
ip access-list list1 permit udp src 172.16.1.1/32 sport any dest 172.16.1.2/32 dport eq 500
!
ppp profile test
  authentication username test@example.com
  authentication password plain test
!
interface GigaEthernet0.0
  no ip address
  encapsulation PPPoE0
  no shutdown
!
interface GigaEthernet1.0
  ip address 192.168.10.254/24
  no shutdown
!
interface PPPoE0
  ip address ipcp
  ppp profile test
  auto-connect
  ip filter list1 1 in
  no shutdown
!
interface IPsec0
  ip address unnumbered
  ip tcp adjust-mss auto
  ipsec map ipsecprof1
  no shutdown
!
!
ip route 172.16.1.1/32 PPPoE0
ip route default IPsec0
!
!
ike proposal ikeprop1
  encryption-algorithm aes256-cbc
  authentication-algorithm hmac-sha1
  lifetime 28800
  dh-group 1024-bit
!
ike policy ikepol1
  mode main
  dpd-keepalive enable 20 3
  proposal ikeprop1
  pre-shared-key plain hogehoge
!
!
ipsec proposal ipsecprop1
  protocol esp enc-algo aes256-cbc auth-algo hmac-sha1-96
  lifetime 28800
!
ipsec policy ipsecpol1
  proposal ipsecprop1
!
ipsec profile ipsecprof1
  mode tunnel
  ipsec policy ipsecpol1
  ike policy ikepol1
  peer 172.16.1.1
!
```

IPsecアグレッシブモード設定例

IPsecのアグレッシブモードにおける基本的な設定を説明します。本設定により、アグレッシブモードでのIPsec通信が可能となります。PPPoE回線とWiMAX端末を利用したトンネルモードを使用した例です。

各コマンドの詳細については、コマンドリファレンスをご参照ください。ルータの基本的な通信設定は、完了している状態からの説明とします。

以下の手順にて設定を行います。

1） IKEプロポーザルの設定
2） IKEポリシーの設定
3） IPsecプロポーザルの設定
4） IPsecポリシーの設定
5） IPsecプロファイルの設定
6） IPsecインタフェースの設定
7） ルーティングの設定
8） NAPT除外の設定

ここでは、装置A（WA1020）にてWiMAX端末を利用し、装置B（WA2021）にてPPPoE回線を利用した、アグレッシブモードの設定を示します。

・装置AのWAN側は動的IPアドレスが払い出され、装置BのWAN側は、固定IPアドレスが払い出されるものとして設定します。

・装置A、装置Bからは、インターネットアクセスが可能なようにNAPTが設定されているものとします。

・装置Aを拠点、装置Bをセンターとし、装置Aから接続する（イニシエータ)構成とします。

※設定に必要となる暗号キーやプロポーザル/ポリシー名等は、事前に決定しておくと設定がスムーズに進みます。

WA1510、WA1511は、WiMAXデータ通信端末の接続をサポートしておりません。
WA1511は、Serial0をサポートしておりません。MobileEthernet0.0を使用してください。

1） IKEプロポーザルの設定

ike proposalコマンドにて、作成するIKE プロポーザル名を指定し、モードを移ります。

暗号化アルゴリズム、認証アルゴリズム、IKE SAの有効時間を設定します。プロポーザル内の各設定を省略した場合は、自動的に初期値が登録されます。

```
WA1020(config)#  ike proposal ikeprop1  [Enter]
WA1020(config-ike-proposal[ikeporp1])# encryption-algorithm aes256-cbc
[Enter]
WA1020(config-ike-proposal[ikeporp1])# authentication-algorithm hmac-sha1
[Enter]
WA1020(config-ike-proposal[ikeporp1])# lifetime 28800 [Enter]
WA1020(config-ike-proposal[ikeprop1])# dh-group 1024-bit [Enter]
WA1020(config-ike-proposal[ikeprop1])# exit [Enter]
WA1020(config)#
```

2） IKEポリシーの設定

ike policyコマンドにて、IKEポリシー名を指定し、モードを移ります。

動作モードの設定（main、aggressive）、IDペイロードの設定、DPD-KeepAliveの設定、 使用するプロポーザルの設定、事前共有鍵の設定を行います。

IDを設定しない場合は、IPアドレスを使用します。

動的IP拠点側はlocal-idを指定してください。固定IP拠点側はremote-idを指定してください。

アグレッシブモードの場合、modeは、aggressiveとします。

l 装置A（WA1020の場合）

```
WA1020(config)# ike policy ikepol1 [Enter]
WA1020(config-ike-policy[ikepol1])# mode aggressive [Enter]
WA1020(config-ike-policy[ikepol1])# local-id key-id wa1020 [Enter]
WA1020(config-ike-policy[ikepol1])# dpd-keepalive enable 20 3 [Enter]
WA1020(config-ike-policy[ikepol1])# proposal ikeprop1 [Enter]
WA1020(config-ike-policy[ikepol1])# pre-shared-key plain hogehoge [Enter]
WA1020(config-ike-policy[ikepol1])# exit[Enter]
```

l 装置B（WA2021の場合）

```
WA2021(config)# ike policy ikepol1 [Enter]
WA2021(config-ike-policy[ikepol1])# mode aggressive [Enter]
WA2021(config-ike-policy[ikepol1])# remote-id key-id wa1020 [Enter]
WA2021(config-ike-policy[ikepol1])# dpd-keepalive enable 20 3 [Enter]
WA2021(config-ike-policy[ikepol1])# proposal ikeprop1 [Enter]
WA2021(config-ike-policy[ikepol1])# pre-shared-key plain hogehoge [Enter]
WA2021(config-ike-policy[ikepol1])# exit[Enter]
WA2021(config)#
```

メモ　回線契約が従量課金の場合、DPD-KeepAliveは課金対象となりますので
送信間隔やリトライ回数にご注意ください。

3） IPsecプロポーザルの設定

ipsec proposalコマンドにて、IPsecプロポーザル名を指定し、モードを移ります。

暗号化アルゴリズム､認証アルゴリズムを設定します｡IPsec SAの有効時間を設定します。
プロポーザル内の各設定を省略した場合は、自動的に初期値が登録されます。

```
WA1020(config)# ipsec proposal ipsecprop1 [Enter]
WA1020(config-ipsec-proposal[ipsecprop1)# protocol esp enc-algo aes256-cbc
auth-algo hmac-sha1-96 [Enter]
WA1020(config-ipsec-proposal[ipsecprop1)# lifetime 28800 [Enter]
WA1020(config-ipsec-proposal[ipsecprop1)# exit [Enter]
WA1020(config)#
```

メモ　IPsec の暗号化アルゴリズムと認証アルゴリズムは複数設定可能です。

4） IPsecポリシーの設定

ipsec policyコマンドにて、IPsecポリシー名を指定し、モードを移ります。

利用するIKEプロポーザル、IPsec SAの自動更新の有無、PFS機能、ESP のセキュリティレベルの設定等をおこないます。ポリシー内の各設定を省略した場合は、自動的に初期値が登録されます。

remote-idとlocal-idは固定IP拠点側と、動的IP拠点側で対になるように指定してください。

l 装置A（WA1020の場合）

```
WA1020(config)# ipsec policy ipsecpol1 [Enter]
WA1020(config-ipsec-policy[ipsecpol1])# proposal ipsecprop1 [Enter]
WA1020(config-ipsec-policy[ipsecpol1])# local-id 192.168.1.0/24 [Enter]
WA1020(config-ipsec-policy[ipsecpol1])# remote-id 192.168.10.0/24 [Enter]
WA1020(config-ipsec-policy[ipsecpol1])# exit [Enter]
WA1020(config)#
```

l 装置B（WA2021の場合）

```
WA2021(config)# ipsec policy ipsecpol1 [Enter]
WA2021(config-ipsec-policy[ipsecpol1])# proposal ipsecprop1 [Enter]
WA2021(config-ipsec-policy[ipsecpol1])# local-id 192.168.10.0/24 [Enter]
WA2021(config-ipsec-policy[ipsecpol1])# remote-id 192.168.1.0/24 [Enter]
WA2021(config-ipsec-policy[ipsecpol1])# exit [Enter]
WA2021(config)#
```

メモ　IPsec SAの自動更新機能は、省略するとrekey enableが設定されます。通信がある間は、自動更新しますが、該当SAで通信が無い場合は、自動更新されません。

５） IPsecプロファイルの設定

ipsec profileコマンドにて、IPsecプロファイル名を指定し、モードを移ります。

利用するIPsecポリシー、利用するIKEポリシー、peer（対向先）、source （SAを確立するインタフェース）を設定します。modeはtunnelを指定します。

アグレッシブモードにおいて、動的IP拠点側は対向拠点のIPアドレスをpeerで指定し、固定IP拠点側はpeer anyを設定してください。

l 装置A（WA1020の場合）

```
WA1020(config)# ipsec profile ipsecprof1 [Enter]
WA1020(config-ipsec-profile[ipsecprof1)# mode tunnel [Enter]
WA1020(config-ipsec-profile[ipsecprof1)# ipsec policy ipsecpol1 [Enter]
WA1020(config-ipsec-profile[ipsecprof1)# ike policy ikepol1 [Enter]
WA1020(config-ipsec-profile[ipsecprof1)# peer 172.16.1.2 [Enter]
WA1020(config-ipsec-profile[ipsecprof1)# exit [Enter]
WA1020(config)#
```

l 装置B（WA2021の場合）

```
WA2021(config)# ipsec profile ipsecprof1 [Enter]
WA2021(config-ipsec-profile[ipsecprof1)# mode tunnel [Enter]
WA2021(config-ipsec-profile[ipsecprof1)# ipsec policy ipsecpol1 [Enter]
WA2021(config-ipsec-profile[ipsecprof1)# ike policy ikepol1 [Enter]
WA2021(config-ipsec-profile[ipsecprof1)# peer any [Enter]
WA2021(config-ipsec-profile[ipsecprof1)# exit [Enter]
WA2021(config)#
```

注意　sourceを省略した場合は、peerに対するルーティングに従い、出力インタフェースのIPアドレスが利用されます。出力インタフェースがオンデマンド設定（no auto-connect）の場合は、sourceを省略することは出来ません。

６） IPsec インタフェースの設定

本製品ではIPsec通信を行うために、専用のIPsecインタフェースを利用します。

IPsecインタフェースの設定を行うため、インタフェースコンフィグモードに移ります。

IPアドレスの設定、利用するIPsecプロファイルの設定、tcp-mss調整の設定を行います。

```
WA1020(config)# interface IPsec0 [Enter]
WA1020(config-IPsec0)# ip address unnumbered [Enter]
WA1020(config-IPsec0)# ipsec map ipsecprof1 [Enter]
WA1020(config-IPsec0)# ip tcp adjust-mss auto [Enter]
WA1020(config-IPsec0)# no shutdown [Enter]
WA1020(config-IPsec0)# exit [Enter]
```

７） ルーティングの設定

IPsec通信を使用する通信をIPsecインタフェースに転送する設定をおこないます。

l 装置A（WA1020の場合）

```
WA1020(config)# ip route 192.168.10.0/24 IPsec0 [Enter]
WA1020(config)# ip route default FastEthernet1.0
```

l 装置B（WA2021の場合）

```
WA2021(config)# ip route 192.168.1.0/24 IPsec0 [Enter]
WA2021(config)# ip route default PPPoE0
```

８） NAPT除外の設定

各装置の出力インタフェース（WA1020:FastEthernet1.0、WA2021:PPPoE0）にNAPT reserve設定を行い、IPsec通信をNAPT変換対象から除外します。

l 装置A（WA1020の場合）

```
WA1020(config)# interface FastEthernet1.0 [Enter]
WA1020(config-FastEthernet1.0)# ip napt enable [Enter]
WA1020(config-FastEthernet1.0)# ip napt reserve udp 500 [Enter]
WA1020(config-FastEthernet1.0)# ip napt reserve esp [Enter]
WA1020(config-FastEthernet1.0)# exit [Enter]
WA1020(config)#
```

l 装置B（WA2021の場合）

```
WA2021(config)# interface PPPoE0 [Enter]
WA2021(config-PPPoE0)# ip napt enable [Enter]
WA2021(config-PPPoE0)# ip napt reserve udp 500 [Enter]
WA2021(config-PPPoE0)# ip napt reserve esp [Enter]
WA2021(config-PPPoE0)# exit [Enter]
WA2021(config)#
```

以下、上記で説明した装置A、装置Bの設定についてIPsec設定を中心に示します。

装置 A

```
!
hostname WA1020
!
!
no wireless-adapter enable
!
interface FastEthernet0.0
  ip address 192.168.1.254/24
  no shutdown
!
interface FastEthernet1.0
  ip address dhcp
  auto-connect
  ip napt enable
  ip napt reserve esp
  ip napt reserve udp 500
  no shutdown
!
!
interface IPsec0
  ip address unnumbered
  ip tcp adjust-mss auto
  ipsec map ipsecprof1
  no shutdown
!
!
ip route 192.168.10.0/24 IPsec0
ip route default FastEthernet1.0
!
ike proposal ikeprop1
  encryption-algorithm aes256-cbc
  authentication-algorithm hmac-sha1
  lifetime 28800
  dh-group 1024-bit
!
!
ike policy ikepol1
  mode aggressive
  local-id key-id wa1020
  dpd-keepalive enable 20 3
  proposal ikeprop1
  pre-shared-key plain hogehoge
!
!
ipsec proposal ipsecprop1
  protocol esp enc-algo aes256-cbc auth-algo hmac-sha1-96
  lifetime 28800
!
ipsec policy ipsecpol1
  local-id 192.168.1.0/24
  remote-id 192.168.10.0/24
  proposal ipsecprop1
!
ipsec profile ipsecprof1
  mode tunnel
  ipsec policy ipsecpol1
  ike policy ikepol1
  peer 172.16.1.2
!
!
```

装置 B

```
hostname WA2021
!
ppp profile test
  authentication username test@example.com
  authentication password plain test
!
!
interface GigaEthernet0.0
  no ip address
  encapsulation PPPoE0
  no shutdown
!
interface GigaEthernet1.0
  ip address 192.168.10.254/24
  no shutdown
!
interface PPPoE0
  ip address ipcp
  ppp profile test
  auto-connect
  ip napt enable
  ip napt reserve esp
  ip napt reserve udp 500
  no shutdown
!
interface IPsec0
  ip address unnumbered
  ip tcp adjust-mss auto
  ipsec map ipsecprof1
  no shutdown
!
!
ip route 192.168.1.0/24 IPsec0
ip route default PPPoE0
!
!
ike proposal ikeprop1
  encryption-algorithm aes256-cbc
  authentication-algorithm hmac-sha1
  lifetime 28800
  dh-group 1024-bit
!
ike policy ikepol1
  mode aggressive
  remote-id key-id wa1020
  dpd-keepalive enable 20 3
  proposal ikeprop1
  pre-shared-key plain hogehoge
!
!
ipsec proposal ipsecprop1
  protocol esp enc-algo aes256-cbc auth-algo hmac-sha1-96
  lifetime 28800
!
ipsec policy ipsecpol1
  local-id 192.168.10.0/24
  remote-id 192.168.1.0/24
  proposal ipsecprop1
!
ipsec profile ipsecprof1
  mode tunnel
  ipsec policy ipsecpol1
  ike policy ikepol1
  peer any
```

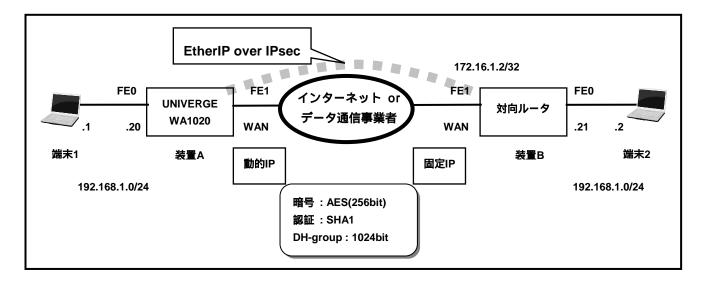
Ether IP over IPsec設定例

IPsecトランスポートモードとEtherIP機能を併用することで、セキュリティを保ったままインターネット間でブリッジ接続を行うことができます。ここではそのための設定を説明します。

各コマンドの詳細については、コマンドリファレンスをご参照ください。

ルータの基本的な通信設定は、完了している状態からの説明とします。

以下の手順にて設定を行います。

1） IKEプロポーザルの設定
2） IKEポリシーの設定
3） IPsecプロポーザルの設定
4） IPsecポリシーの設定
5） IPsecプロファイルの設定
6） WAN側インタフェースの設定
7） ブリッジの設定
8） EtherIPの設定

装置AでWiMAXを使用した場合の設定例を示します。装置Bは固定IPアドレスとします。

ここでは装置Aの設定例を中心に説明します。装置Bは装置Aと対向できるような設定としてください。

※設定に必要となる暗号キーやプロポーザル/ポリシー名等は、事前に決定しておくと設定がスムーズに進みます。

装置AのインタフェースFastEthernet1.0と装置BのWAN側アドレスを終端アドレスとするIPsec（トランスポートモード）接続の設定をします。次にブリッジ機能を有効にしてFastEthernet1.0とEtherIP0インタフェースを同一ブリッジグループに設定します。EtherIP0インタフェースにカプセル化の際のソースアドレス、宛先アドレスを設定します。

注意　ソフトウェアバージョン 3.2 以下では、EtherIP 機能を使用した場合、Ethernet の最大フレーム長が 1518byte に制限されているため、VLAN タグ付きの Ethernet フレームの最大長(1522byte)を転送できません。ソフトウェアバージョン 4.0 以降は 1522byte まで転送が可能です。

注意　WA1510、WA1511は、WiMAXデータ通信端末の接続をサポートしておりません。WA1511は、Serial0をサポートしておりません。MobileEthernet0.0を使用してください。

以下、IPsec、EtherIP関連のコンフィグを中心に、順に説明します。

1） IKEプロポーザルの設定

ike proposalコマンドにて、作成するIKE プロポーザル名を指定し、モードを移ります。

暗号化アルゴリズム、認証アルゴリズム、IKE SAの有効時間を設定します。プロポーザル内の各設定を省略した場合は、自動的に初期値が登録されます。

```
WA1020(config)#  ike proposal ikeprop1 [Enter]
WA1020(config-ike-proposal[ikeprop1])# encryption-algorithm aes256-cbc [Enter]
WA1020(config-ike-proposal[ikeprop1])# authentication-algorithm hmac-sha1  [Enter]
WA1020(config-ike-proposal[ikeprop1])# lifetime 28800 [Enter]
WA1020(config-ike-proposal[ikeprop1])# dh-group 1024-bit [Enter]
WA1020(config-ike-proposal[ikeprop1])# exit [Enter]
WA1020(config)#
```

2） IKEポリシーの設定

ike policyコマンドにて、IKEポリシー名を指定し、モードを移ります。

動作モードの設定（main、aggressive）、IDペイロードの設定、DPD-KeepAliveの設定、 使用するプロポーザルの設定、事前共有鍵の設定を行います。

IDを設定しない場合は、IPアドレスを使用します。

動的IP拠点側はlocal-idを指定してください。固定IP拠点側はremote-idを指定してください。

アグレッシブモードの場合、modeはaggressiveを指定します。

```
WA1020(config)# ike policy ikepol1 [Enter]
WA1020(config-ike-policy[ikepol1])# mode aggressive [Enter]
WA1020(config-ike-policy[ikepol1])# local-id key-id wa1020 [Enter]
WA1020(config-ike-policy[ikepol1])# dpd-keepalive enable 20 3 [Enter]
WA1020(config-ike-policy[ikepol1])# proposal ikeprop1 [Enter]
WA1020(config-ike-policy[ikepol1])# pre-shared-key plain hogehoge [Enter]
WA1020(config-ike-policy[ikepol1])# exit[Enter]
WA1020(config)#
```

メモ　回線契約が従量課金の場合、DPD-KeepAliveは課金対象となりますので送信間隔やリトライ回数にご注意ください。

3） IPsecプロポーザルの設定

ipsec proposalコマンドにて、IPsecプロポーザル名を指定し、モードを移ります。

暗号化アルゴリズム、認証アルゴリズムを設定します。IPsec SAの有効時間を設定します。プロポーザル内の各設定を省略した場合は、自動的に初期値が登録されます。

```
WA1020(config)# ipsec proposal ipsecprop1 [Enter]
WA1020(config-ipsec-proposal[ipsecprop)# protocol esp enc-algo aes256-cbc
auth-algo hmac-sha1-96 [Enter]
WA1020(config-ipsec-proposal[ipsecprop)# lifetime 28800 [Enter]
WA1020(config-ipsec-proposal[ipsecprop)# exit [Enter]
WA1020(config)#
```

メモ　IPsec の暗号化アルゴリズムと認証アルゴリズムは複数設定できます。

4） IPsecポリシーの設定

ipsec policyコマンドにて、IPsecポリシー名を指定し、モードを移ります。

利用するIKEプロポーザル、IPsec SAの自動更新の有無、PFS機能、ESP のセキュリティレベルの設定等をおこないます。ポリシー内の各設定を省略した場合は、自動的に初期値が登録されます。

remote-idとlocal-idは固定IP拠点側と、動的IP拠点側で対になるように指定してください。

```
WA1020(config)# ipsec policy ipsecpol1 [Enter]
WA1020(config-ipsec-policy[ipsecpol1])# local-id 192.168.1.20/32 [Enter]
WA1020(config-ipsec-policy[ipsecpol1])# remote-id 192.168.1.21/32 [Enter]
WA1020(config-ipsec-policy[ipsecpol1])# proposal ipsecprop1 [Enter]
WA1020(config-ipsec-policy[ipsecpol1])# exit [Enter]
WA1020(config)#
```

メモ　IPsec SAの自動更新機能は、省略するとrekey enableが設定されます。通信がある間は、自動更新しますが、該当SAで通信が無い場合は、自動更新されません。

5） IPsecプロファイルの設定

ipsec profileコマンドにて、IPsecプロファイル名を指定し、モードを移ります。

使用するモード、利用するIPsecポリシー、利用するIKEポリシー、peer（対向先）、source（SAを確立するインタフェース）を設定します。modeはtransportを指定します。

アグレッシブモードにおいて、動的IP拠点側は対向拠点のIPアドレスをpeerで指定し、

固定IP拠点側はpeer anyを設定してください。

```
WA1020(config)# ipsec profile ipsecprof1 [Enter]
WA1020(config-ipsec-profile[ipsecprof1)# mode transport [Enter]
WA1020(config-ipsec-profile[ipsecprof1)# ipsec policy ipsecpol1 [Enter]
WA1020(config-ipsec-profile[ipsecprof1)# ike policy ikepol1 [Enter]
WA1020(config-ipsec-profile[ipsecprof1)# peer 172.16.1.2 [Enter]
WA1020(config-ipsec-profile[ipsecprof1)# source FastEthernet1.0 [Enter]
WA1020(config-ipsec-profile[ipsecprof1)# exit [Enter]
WA1020(config)#
```

６）ＷＡＮ側インタフェースの設定

トランスポートモードでは物理インタフェースにIPsecプロファイルをマップすることで、そのインタフェースで送受信されるパケットを暗号化の対象とします。

インタフェースの設定を行うため、インタフェースコンフィグモードに移ります。

IPアドレスの設定、利用するIPsecプロファイルの設定などを行います。

```
WA1020(config)# interface FastEthernet1.0 [Enter]
WA1020(config-FastEthernet1.0)# ip address dhcp [Enter]
WA1020(config-FastEthernet1.0)# ipsec map ipsec_prof1 [Enter]
WA1020(config-FastEthernet1.0)# no shutdown [Enter]
WA1020(config-FastEthernet1.0)# exit [Enter]
WA1020(config)#
```

7） ブリッジの設定

グローバルコンフィグでブリッジグループを有効にします。FastEthernet0.0インタフェースコンフィグモードでブリッジグループを設定します。（EtherIP0インタフェースのブリッジの設定は後で行います）

```
WA1020(config)# bridge ieee enable [Enter]
WA1020(config)# interface FastEthernet0.0
WA1020(config-FastEthernet0.0)# bridge ieee 1 [Enter]
WA1020(config-FastEthernet0.0)# exit [Enter]
WA1020(config)#
```

8） EtherIPインタフェースの設定

EtherIP0のインタフェースコンフィグモードで、ブリッジグループを有効にし、peer とsourceアドレスを設定します。peerは装置BのWAN側アドレスです。

また、IPsec over EtherIPのカプセル化により、TCP/IPパケットのフラグメントを防ぐために、mss調整のための設定を推奨します。

```
WA1020(config)# interface EtherIP0 [Enter]
WA1020(config-EtherIP0)# bridge ieee 1 [Enter]
WA1020(config-EtherIP0)# ether-ip peer 172.16.1.2 [Enter]
WA1020(config-EtherIP0)# ether-ip source FastEthernet1.0 [Enter]
WA1020(config-EtherIP0)# ether-ip adjust-ip-tcp-mss 1286 [Enter]
WA1020(config-EtherIP0)# exit [Enter]
WA1020(config)#
```

以下、上記で説明した装置Aの全体の設定を示します。

装置 A

```
hostname WA1020-1
!
no wireless-adapter enable
!
bridge ieee enable
!
interface FastEthernet0.0
  ip address 192.168.1.20/24
  bridge ieee 1
  no shutdown
!
interface FastEthernet1.0
  ip address dhcp
  ipsec map ipsec_prof1
  no shutdown
!
interface IPsec0
  ip address unnumbered
  no shutdown
!
interface IPsec1
  no ip address
  shutdown
!
interface EtherIP0
  bridge ieee 1
  ether-ip peer 172.16.1.2
  ether-ip source FastEthernet1.0
  ether-ip adjust-ip-tcp-mss 1286
  no shutdown
!
!
ip route default FastEthernet1.0
!
ike proposal ikeprop1
  encryption-algorithm aes256-cbc
  authentication-algorithm hmac-sha1
  lifetime 28800
  dh-group 1024-bit
!
ike policy ikepol1
  mode aggressive
  local-id key-id wa1020-1
  proposal ikeprop1
  pre-shared-key plain hogehoge
!
!
ipsec proposal ipsecprop1
  protocol esp enc-algo aes256-cbc auth-algo hmac-sha1-96
  lifetime 300 100000
!
ipsec policy ipsecpol1
  local-id 192.168.1.20/32
  remote-id 192.168.1.21/32
  proposal ipsecprop1
!
ipsec profile ipsecprof1
  mode transport
  ipsec policy ipsecpol1
  ike policy ikepol1
  source FastEthernet1.0
  peer 172.16.1.2
!
```

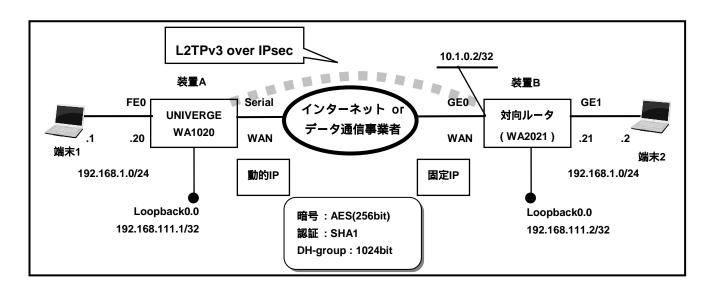
L2TPv3 over IPsec設定例

IPsecトンネルモードとL2TPv3機能を併用することで、セキュリティを保ったままインターネット間でブリッジ接続を行うことができます。ここではそのための設定を説明します。

各コマンドの詳細については、コマンドリファレンスをご参照ください。

ルータの基本的な通信設定は、完了している状態からの説明とします。

以下の手順にて設定を行います。

1） IKEプロポーザルの設定
2） IKEポリシーの設定
3） IPsecプロポーザルの設定
4） IPsecポリシーの設定
5） IPsecプロファイルの設定
6） IPsecインタフェースの設定
7） WAN側インタフェースの設定
8） ブリッジの設定
9） L2TPv3の設定
10）ルーティングの設定

装置AでSerialを使用した場合の設定例を示します。装置Bは固定IPアドレスとします。

ここでは装置Aの設定例を中心に説明します。装置Bは装置Aと対向できるような設定としてください。

※設定に必要となる暗号キーやプロポーザル/ポリシー名等は、事前に決定しておくと設定がスムーズに進みます。

装置AのWAN側インタフェースと装置BのWAN側アドレスを終端アドレスとするIPsec（トンネルモード）接続の設定をします。次にブリッジ機能を有効にしてLAN側インタフェースとL2TP0インタフェースを同一ブリッジグループに設定します。L2TP0インタフェースにカプセル化の際のソースアドレス、宛先アドレスを設定します。

注意　WA1510、WA1511は、WiMAXデータ通信端末の接続をサポートしておりません。WA1511は、Serial0をサポートしておりません。MobileEthernet0.0を使用してください。

以下はIPsec関連の設定です。

コンフィグの設定方法については、IPsecアグレッシブモード設定例を参照願います。

１） IKEプロポーザルの設定

２） IKEポリシーの設定

３） IPsecプロポーザルの設定

４） IPsecポリシーの設定

５） IPsecプロファイルの設定

６） IPsecインタフェースの設定

続いて、以下を実施します。

７） WAN側インタフェースの設定

コンフィグの設定方法については、ルータモード設定例（HSPAの場合）を参照願います。

８） ブリッジの設定

グローバルコンフィグでブリッジグループを有効にします。FastEthernet0.0インタフェースコンフィグモードでブリッジグループを設定します。（L2TP0インタフェースのブリッジの設定は後で行います）

```
WA1020(config)# bridge ieee enable [Enter]
WA1020(config)# interface FastEthernet0.0
WA1020(config-FastEthernet0.0)# bridge ieee 1 [Enter]
WA1020(config-FastEthernet0.0)# exit [Enter]
WA1020(config)#
```

９） L2TPインタフェースの設定

L2TP0のインタフェースコンフィグモードで、ブリッジグループを有効にし、peer と sourceアドレスを設定します。peerに装置BのLoopback0.0アドレス、sourceに装置AのLoopback0.0インタフェースを指定します。

また、L2TP over IPsec のカプセル化により、TCP/IPパケットのフラグメントを防ぐために、mss調整のための設定を推奨します。

```
WA1020(config)# interface L2TP0 [Enter]
WA1020(config-EtherIP0)# bridge ieee 1 [Enter]
WA1020(config-EtherIP0)# l2tp peer 192.168.111.2 [Enter]
WA1020(config-EtherIP0)# l2tp source Loopback0.0 [Enter]
WA1020(config-EtherIP0)# l2tp adjust-ip-tcp-mss 1312 [Enter]
WA1020(config-EtherIP0)# exit [Enter]
WA1020(config)# interface loopback0.0 [Enter]
WA1020(config-EtherIP0)# ip address 192.168.111.1/32 [Enter]
WA1020(config-EtherIP0)# exit [Enter]
```

１０） ルーティングの設定

L2TPv3でカプセル化したIPv4パケットをIPsecインタフェースにルーティングするための設定を行います。

```
WA1020(config)# ip route default Serial0 [Enter]
WA1020(config)# ip route 192.168.111.2/32 IPsec0 [Enter]
WA1020(config)# exit [Enter]
```

以下、上記で説明した装置A、装置Bの設定を示します。

装置 A

```
hostname WA1020
!
no wireless-adapter enable
!
ppp profile test
  authentication username test@example.com
  authentication password plain test
!
bridge ieee enable
!
interface FastEthernet0.0
  ip address 192.168.1.20/24
  bridge ieee 1
  no shutdown
!
interface L2TP0
  l2tp encapsulation l2tpv3
  l2tp adjust-ip-tcp-mss 1312
  l2tp source Loopback0.0
  l2tp peer 192.168.111.2
  bridge ieee 1
  no shutdown
!
interface Serial0
  ip address ipcp
  ppp profile test
  mobile id IP 1 net.example.com
  mobile number *99***CID#
  auto-connect
  no shutdown
!
interface Loopback0.0
  ip address 192.168.111.1/32
  no shutdown
!
interface IPsec0
  ip address unnumbered
  ipsec map ipsecprof1
  no shutdown
!
ip route default Serial0
ip route 192.168.111.2/32 IPsec0
!
ike proposal ikeprop1
  encryption-algorithm aes256-cbc
  authentication-algorithm hmac-sha1
  lifetime 28800
  dh-group 1024-bit
!
ike policy ikepol1
  mode aggressive
  local-id key-id wa1020
  dpd-keepalive enable ph1 20 3
  proposal ikeprop1
  pre-shared-key plain hogehoge
!
ipsec proposal ipsecprop1
  protocol esp enc-algo aes256-cbc auth-algo hmac-sha1-96
  lifetime 28800
!
ipsec policy ipsecpol1
  local-id 192.168.111.1/32
  remote-id 192.168.111.2/32
  proposal ipsecprop1
!
ipsec profile ipsecprof1
  mode tunnel
  ipsec policy ipsecpol1
  ike policy ikepol1
  peer 10.1.0.2
```

装置 B

```
hostname WA2021
!
ppp profile test
  authentication username test@example.com
  authentication password plain test
!
bridge ieee enable
!
interface GigaEthernet0.0
  no ip address
  encapsulation PPPoE0
  no shutdown
!
interface GigaEthernet1.0
  ip address 192.168.1.21/24
  bridge ieee 1
  no shutdown
!
interface L2TP0
  l2tp encapsulation l2tpv3
  l2tp adjust-ip-tcp-mss 1312
  l2tp source Loopback0.0
  l2tp peer 192.168.111.1
  bridge ieee 1
  no shutdown
!
interface PPPoE0
  ip address ipcp
  ppp profile test
  auto-connect
  no shutdown
!
interface Loopback0.0
  ip address 192.168.111.2/32
  no shutdown
!
interface IPsec0
  ip address unnumbered
  ipsec map ipsecprof1
  no shutdown
!
ip route default PPPoE0
ip route 192.168.111.1/32 IPsec0
!
ike proposal ikeprop1
  encryption-algorithm aes256-cbc
  authentication-algorithm hmac-sha1
  lifetime 28800
  dh-group 1024-bit
!
ike policy ikepol1
  mode aggressive
  remote-id key-id wa1020
  dpd-keepalive enable ph1 20 3
  proposal ikeprop1
  pre-shared-key plain hogehoge
!
ipsec proposal ipsecprop1
  protocol esp enc-algo aes256-cbc auth-algo hmac-sha1-96
  lifetime 28800
!
ipsec policy ipsecpol1
  local-id 192.168.111.2/32
  remote-id 192.168.111.1/32
  proposal ipsecprop1
!
ipsec profile ipsecprof1
  mode tunnel
  ipsec policy ipsecpol1
  ike policy ikepol1
  peer any
```

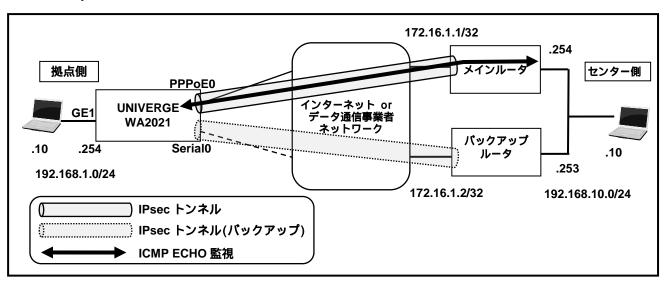
ネットワークモニタ機能設定例

ネットワークモニタ機能の基本的な設定を説明します。ここでは2箇所へのIPsec（アグレッシブモード）の接続を行い、メインルータへの通信が不通になった場合、バックアップルータに切り替える設定を行います。

各コマンドの詳細については、コマンドリファレンスをご参照ください。

2箇所の接続先へのIPsec（アグレッシブモード）の設定まで完了している状態からの説明とします。

以下の手順にて設定を行います。

1） ルーティング設定
2） ネットワークモニタグループ（イベント）の設定
3） ネットワークモニタグループ（アクション）の設定
4） 対向ルータからのホスト監視パケットへの応答指定の設定
 (ソフトウェアバージョン4.0以降)
5） ネットワークモニタの開始
6） バックアップ回線のパラメータ調整

UNIVERGE WA2021を利用し、WAN側インタフェースとしてPPPoE（GE0）と、HSPAを使用する場合の例です。

・IPsec0 にてメインルータへ接続し、IPsec1にてバックアップルータへ接続します。

・ネットワークモニタ機能にて、監視ホストへの到達性が失われた際に、メインルータへの経路を削除しバックアップ経路を追加します。また、利用するプロキシDNSサーバの切り替えも設定します。

・UNIVERGE WA2021側の設定のみ説明します。ネットワークモニタ機能による冗長構成の場合、対向ルータでも同様の冗長切り替えの設定が必要になります。

注意　WA1511は、Serial0をサポートしておりません。MobileEthernet0.0を使用してください。

1） ルーティングの設定

対向LAN側へのメイン回線を利用した経路を設定します。

また、デフォルトルートと対向ルータへの各ルートも設定します。

```
WA2021(config)# ip route 192.168.2.0/24 IPsec0
WA2021(config)# ip route default PPPoE0
WA2021(config)# ip route 172.16.1.1/32 PPPoE0
WA2021(config)# ip route 172.16.1.2/32 Serial0
```

注意　ネットワークモニタ機能と、フローティングスタティック機能の同時動作は出来ません。ルートの切り替えは、actionによるルートの削除/追加を行う必要があります。

2） ネットワークモニタグループ（イベント）の設定

network-monitorコマンドにて、作成するネットワークモニタグループ名を指定し、モードを移ります。

監視対象のIPアドレスを対向LAN側のIPアドレスとし、出力インタフェースを設定します。

送信元アドレスは、対向からの折り返しのルーティングが可能となるように、WA2021のLAN側を指定します。

```
WA2021(config)# network-monitor monitor1 [Enter]
WA2021(config-netmon[monitor1])# event ip unreach-host 192.168.10.254
interface IPsec0 source GigaEthernet1.0 [Enter]
WA2021(config-netmon[monitor1])#
```

次にイベント発生監視インターバル、イベント復旧監視インターバル、イベント発生回数、イベント復旧回数、スタートアップディレイ時間を設定します。各設定を省略した場合は、自動的に初期値が登録されます。

```
WA2021(config-netmon[monitor1])# monitor interval occurrence 30 5 [Enter]
WA2021(config-netmon[monitor1])# monitor interval restorer 10 [Enter]
WA2021(config-netmon[monitor1])# monitor counter occurrence 10 [Enter]
WA2021(config-netmon[monitor1])# monitor counter restorer 5 [Enter]
WA2021(config-netmon[monitor1])# monitor startup-delay 60 [Enter]
WA2021(config-netmon[monitor1])#
```

3） ネットワークモニタグループ（アクション）の設定

イベント発生時に実行するアクションを設定します。

まず、対向のLAN側への経路として、IPsec0へのスタティックルートを削除し、IPsec1へのスタティクルートを追加します。デフォルトルートもPPPoEからSerial0に切り替えます。

```
WA2021(config-netmon[monitor1])# action 10 route-del 192.168.10.0/24 IPsec0
route-add 192.168.10.0/24 IPsec1 [Enter]
WA2021(config-netmon[monitor1])# action 11 route-del 0.0.0.0/0 PPPoE0
route-add 0.0.0.0/0 Serial0 [Enter]
WA2021(config-netmon[monitor1])#
```

次に、プロキシDNS機能を利用する場合、各回線から付与されるDNSサーバを利用する必要があります。回線の冗長化を行う場合は、ネットワークモニタ機能にて、プロキシDNSサーバの設定を変更するactionを指定します。

```
WA2021(config-netmon[monitor1])# action 20 pdns-server-del PPPoE0 ipcp [Enter]
WA2021(config-netmon[monitor1])# action 30 pdns-server-add Serial0 ipcp [Enter]
```

最後に、バックアップ回線を利用したことを示すBAK LEDを点灯させるアクションを追加します。（BAK LEDがあるのはWA2020とWA2021です）

また、バックアップ側のSerial0で利用するデータ通信端末のauto-recovery機能を有効にするアクションを追加します。データ通信端末はUSB0に接続しているものとします。

```
WA2021(config-netmon[monitor1])# action 40 BAK-LED-on [Enter]
WA2021(config-netmon[monitor1])# action 50 auto-recovery interface Serial0[Enter]
WA2021(config-netmon[monitor1])# action 60 auto-recovery device usb0
WA2021(config-netmon[monitor1])# exit [Enter]
WA2021(config)#
```

4） 対向ルータからのホスト監視パケットへの応答指定の設定
(ソフトウェアバージョン4.0以降)

対向ルータ側でWA2021へICMP ECHOによるホスト監視を行う場合は、その応答を受信インタフェースから返信するための設定を行います。

本設定を行わないと、対向ルータへの応答が受信とは別の経路から送信され、対向ルータ側のホスト監視機能が正常に動作しない場合があります。

```
WA1020(config)# monitor-group monitor1 directed-response [Enter]
WA1020(config)#
```

5） ネットワークモニタの開始

monitor-groupコマンドでネットワークモニタ機能を開始します。スタートアップディレイ時間経過後から監視が開始されます。

```
WA1020(config)# monitor-group monitor1 enable [Enter]
WA1020(config)#
```

6） バックアップ回線のパラメータ調整

バックアップ回線はデータ通信端末のパケット通信量を低減させるため、オンデマンド通信の設定を行います。また、メイン回線の復旧に伴い、バックアップ側回線を速やかに切断するためのパラメータ調整を行います。

・Serial0のオンデマンド設定、idle-timer設定

・ike / ipsec のLifetimeの設定

```
WA2021(config)# interface Serial0 [Enter]
WA2021(config-Serial0)# no auto-connect [Enter]
WA2021(config-Serial0)# idle-time timer 60 [Enter]
WA2021(config-Serial0)# exit [Enter]
WA2021(config)# ike proposal ikeprop2 [Enter]
WA2021(config-ike-proposal[ikeprop2])# lifetime 300 [Enter]
WA2021(config-ike-proposal[ikeprop2])# exix [Enter]
WA2021(config)# ipsec proposal ipsecprop2 [Enter]
WA2021(config-ipsec-proposal[ipsecprop2])# lifetime 300 [Enter]
WA2021(config-ipsec-proposal[ipsecprop2])# exit [Enter]
WA2021(config)#
```

メモ　ネットワークモニタグループは最大4個まで登録できます。ソフトウェアバージョン5.0からは、モニタグループ最大16個まで登録できます。グループあたりイベントは1件、アクションは20件まで登録できます。

注意　ネットワークモニタ機能を使用する場合は、以下の点に注意してください。

- アクションコマンドで同じ宛先ネットワークへのルート情報の追加、削除の設定をする場合には、1つのアクションコマンド内で設定するか、 route-del を route-addよりも小さなシーケンスナンバーで設定してください。逆に設定すると、アクション実行時に正常にスタティックルート設定が行われません。

- ソフトウェアバージョン4.1.4未満では、同じ宛先ネットワークへのルート情報の追加、削除を、2つ以上のネットワークモニタグループで設定しないでください。アクション実行時に正常にスタティックルートの設定が行われない場合があります。

- フローティングスタティックルーティング機能と、ネットワークモニタ機能のスタティックルート削除/追加アクションを併用することはできません。経路変更によるバックアップを行う場合には、どちらか片方の機能のみの設定をしてください。

- ICMP ECHOパケットの応答を別の経路で受信しても、監視は成功と判定します。
  応答パケットが正しい経路で送信されるようなネットワーク構成、対向ルータ

の設定をしてください。

- ルーティングによる迂回の動作になりますので、対向側のルータでも迂回経路の設定が必要となります。適切な迂回／復旧経路の設定を対向ルータに設定してください。

- スタティックルートの追加/削除アクションの設定において、例えば

  action 10 route-del 192.168.2.0/24 IPsec0

  と設定した場合、アクション発動時に 192.168.2.0/24宛てのルートのネクストホップがIPsec0以外であっても、ルート情報が削除されてしまいますので、ご注意ください。

- スタティックルートの追加または削除のアクションが設定されたネットワークモニタグループが登録されている状態でそのモニタグループのアクションが１回でも実行された場合、ネットワークモニタで追加/削除した宛先ネットワーク/ホスト宛のスタティックルートをip routeコマンドで設定または削除しても､正しく反映されません。
  ネットワークモニタのアクションでルートを制御しているときに､CLIで同一のルートの追加や削除を行わないでください。

- イベント発生中(アクション発動中)はアクションの追加/削除を行うことができません。当該グループの監視動作を停止(no monitor-group コマンド)をしてからアクションの追加/削除を行ってください。

- ソフトウェアバージョン4.0未満では､監視先ホストへのルート情報をアクションで追加、削除を設定しないでください。正常にホスト監視が行えなくなります。
  以下のような設定はできません。

  event ip unreach-host 192.168.10.254 interface IPsec0 source GigaEthernet1.0
  action 10 route-del 192.168.10.254/32 IPsec0 route-add 192.168.10.254/32 IPsec1

  追加、削除するスタティックルートの宛先がネットワーク指定の場合は、そのネットワークに監視先ホストが含まれていてもかまいません。(下記はOK)

  action 10 route-del 192.168.10.0/24 IPsec0 route-add 192.168.10.0/24 IPsec1

以下、上記で説明した WA2021 のネットワークモニタ設定を示します。

```
!
hostname WA2021
!
!
ppp profile test1
  authentication username test1
  authentication password plain test1
!
ppp profile test2
  authentication username test2
  authentication password plain test2
!
interface GigaEthernet0.0
  no ip address
  encapsulation PPPoE0
  no shutdown
!
interface GigaEthernet1.0
  ip address 192.168.1.254/24
  no shutdown
!
interface PPPoE0
  ip address ipcp
  ppp profile test1
  auto-connect
  ip napt enable
  ip napt reserve esp
  ip napt reserve udp 500
  no shutdown
!
interface Serial0
  ip address ipcp
  ppp profile test2
  ip napt enable
  ip napt reserve esp
  ip napt reserve udp 500
  mobile id PPP 1 net.example.com
  mobile number *99***CID#
  no auto-connect
  idle-time timer 60
  no shutdown
!
interface IPsec0
  ip address unnumbered
  ip tcp adjust-mss auto
  ipsec map ipsecprof1
  no shutdown
!
interface IPsec1
  ip address unnumbered
  ip tcp adjust-mss auto
  ipsec map ipsecprof2
  no shutdown
!
!
ip route default PPPoE0
ip route 172.16.1.1/32 PPPoE0
ip route 172.16.1.2/32 Serial0
ip route 192.168.10.0/24 IPsec0
!
network-monitor monitor1
  monitor interval occurrence 30 5
  monitor interval restorer 10
  monitor counter occurrence 10
  monitor counter restorer 5
  monitor startup-delay 60
  event ip unreach-host 192.168.10.254 interface IPsec0 source GigaEthernet1.0
  action 10 route-del 192.168.10.0/24 IPsec0 route-add 192.168.10.0/24 IPsec1
  action 11 route-del 0.0.0.0/0 PPPoE0 route-add 0.0.0.0/0 Serial0
  action 20 pdns-server-del PPPoE0 ipcp
  action 30 pdns-server-add Serial0 ipcp
  action 40 BAK-LED-on
!
```

```
monitor-group monitor1 enable
monitor-group monitor1 directed-response
!
proxy-dns enable
proxy-dns server default PPPoE0 ipcp
!

ike proposal ikeprop1
  encryption-algorithm aes256-cbc
  authentication-algorithm hmac-sha1
  lifetime 28800
  dh-group 1024-bit
!
ike proposal ikeprop2
  encryption-algorithm aes256-cbc
  authentication-algorithm hmac-sha1
  lifetime 300
  dh-group 1024-bit
!
ike policy ikepol1
  mode aggressive
  local-id key-id wa1020
  dpd-keepalive enable 20 3
  proposal ikeprop1
  pre-shared-key plain hogehoge
!
ike policy ikepol2
  mode aggressive
  local-id key-id wa1020
  dpd-keepalive enable 20 3
  proposal ikeprop2
  pre-shared-key plain hogehoge
!
!
ipsec proposal ipsecprop1
  protocol esp enc-algo aes256-cbc auth-algo hmac-sha1-96
  lifetime 28800
!
ipsec proposal ipsecprop2
  protocol esp enc-algo aes256-cbc auth-algo hmac-sha1-96
  lifetime 300
!
ipsec policy ipsecpol1
  local-id 192.168.1.0/24
  remote-id 192.168.10.0/24
  proposal ipsecprop1
!
ipsec policy ipsecpol2
  local-id 192.168.1.0/24
  remote-id 192.168.10.0/24
  proposal ipsecprop2
!
ipsec profile ipsecprof1
  mode tunnel
  ipsec policy ipsecpol1
  ike policy ikepol1
  peer 172.16.1.1
!
ipsec profile ipsecprof2
  mode tunnel
  ipsec policy ipsecpol2
  ike policy ikepol2
  source Serial0
  peer 172.16.1.2
!
```

IPsec peer FQDN設定例

WAシリーズ専用Dynamic DNSサービスを利用して、IPsecのメインモードでpeerコマンドのFQDNオプションを使用した場合の設定を説明します（メインモードの利用はソフトウェアバージョン4.0から、ソフトウェアバージョン3.2以前はアグレッシブモードのみ利用可能）。

本設定により、WAN回線のIPアドレスが接続毎に変化する契約の場合でもIPsec通信が可能となります。以下は、PPPoEとWiMAXでトンネルモードを使用した設定例です。本章はIPsec peer FQDN関連の設定のみ記載します。その他のIPsecの設定は、前述の「IPsecメインモード設定例」をご参照ください。

各コマンドの詳細については、コマンドリファレンスをご参照ください。

以下の手順にて設定を行います。

1） IKEポリシーのメインモード、DPD KeepAliveの設定
2） Dynamic DNSの設定
3） WAシリーズ専用Dynamic DNSサービスの登録確認
4） IPsecプロファイルのpeer FQDN設定
5） プロキシDNSの設定
6） IPsecプロファイルの格納確認

IKEポリシーのmode設定は、mainとします。また、動的IPアドレスの対向のため、物理インタフェースではIPアドレスによるフィルタ設定はできません。代わりにNAPTを利用してください。

※設定に必要となる暗号キーやプロポーザル/ポリシー名等は、事前に決定しておくと設定がスムーズに進みます。

メモ　WAシリーズ専用Dynamic DNSサービスをご利用になる場合のFQDNは装置固有で、任意のFQDNを指定することは出来ません。FQDNは、show ddnsコマンドで確認できます。詳細は「コマンドリファレンス」をご参照ください。

メモ　その他のDynmic DNSサービスを利用するには、あらかじめ、ご利用となるDDNSサービスへのユーザ登録、使用するドメイン名の登録をしてください。

注意　装置A及び装置Bに、IKEポリシーのDPD KeepAliveの設定をすることを推奨します。DPD KeepAliveの設定がされないと、一方の装置で再起動等によりSAが消失した場合、rekeyによってSAが更新されるまで通信ができません。

注意　PeerFQDNのメインモードはソフトウェアバージョン4.0から利用できます。ソフトウェアバージョン3.2以前ではアグレッシブモードのみの対応です。

注意　WA1510、WA1511は、WiMAXデータ通信端末の接続をサポートしておりません。WA1511は、Serial0をサポートしておりません。MobileEthernet0.0を使用してください。

1） IKEポリシーのメインモード、DPD KeepAliveの設定

装置A、Bにて、IKEポリシーのメインモードのmode設定を行います。

装置A、Bにて、DPD KeepAliveの設定を行います。

ここでは装置Aの設定例を示します。

```
WA1020(config)# ike policy ikepol1 [Enter]
WA1020(config-ipsec-policy[ikepol1])# mode main [Enter]
WA1020(config-ipsec-policy[ikepol1])# dpd-keepalive enable 20 3 [Enter]
WA1020(config-ipsec-policy[ikepol1])# exit [Enter]
WA1020(config)#
```

2） Dynamic DNSの設定

装置A、Bにて、動的なIPアドレスをFQDNを利用し、DNSにより解決するため、Dynamic DNSを使用します。

ddnsコマンドにて、Dynamic DNSの動作設定を行います。

アカウントの登録、IPアドレス登録間隔、Dynamic DNS機能の有効化を設定します。登録間隔を省略した場合は、自動的に初期値が登録されます。

l 装置A（WA1020の場合）

```
WA1020(config)# ddns account waddns source-ip auto[Enter]
WA1020(config)# ddns enable [Enter]
WA1020(config)#
```

l 装置B（WA2021の場合）

```
WA2021(config)# ddns account waddns source-ip auto[Enter]
WA2021(config)# ddns enable [Enter]
WA2021(config)#
```

3） WAシリーズ専用Dynamic DNSサービスの登録確認

登録したFQDNを指定し、以下のようにしてIPアドレスが解決されることを確認します。

インターネットに接続できるPC等から、show ddnsコマンドで表示されるFQDNのIPアドレスをnslookupにて確認し、show interfaceコマンドで表示されるIPアドレスと同じであることを確認します。

4） IPsecプロファイルのpeer FQDN 設定

装置A、Bにて、ipsec profile コマンドにてIPsecプロファイル名を指定し、モードを移ります。peerコマンドにて、装置A、BのFQDNを登録します。

l 装置A（WA1020の場合）

```
WA1020(config)# ipsec profile ipsecprof1 [Enter]
WA1020(config-ipsec-profile[ipsecprof1)# peer wa2*********.waddns.com[Enter]
WA1020(config-ipsec-profile[ipsecprof1)# exit [Enter]
WA1020(config)#
```

l 装置B（WA2021の場合）

```
WA2021(config)# ipsec profile ipsecprof1 [Enter]
WA2021(config-ipsec-profile[ipsecprof1)# peer wa1*********.waddns.com[Enter]
WA2021(config-ipsec-profile[ipsecprof1)# exit [Enter]
WA2021(config)#
```

5） プロキシDNSの設定

DNSサーバへ名前(FQDN)解決の動作を行うプロキシDNSの設定をおこないます。

proxy-dnsコマンドにて、装置A、BでFQDNの名前解決のリゾルバを動作させます。

l 装置A（WA1020の場合）

```
WA1020(config)# proxy-dns server default FastEthernet1.0 dhcp [Enter]
WA1020(config)# proxy-dns enable [Enter]
WA1020(config)#
```

l 装置B（WA2021の場合）

```
WA2021(config)# proxy-dns server default PPPoE0 ipcp [Enter]
WA2021(config)# proxy-dns enable [Enter]
WA2021(config)#
```

6） IPsecプロファイルの格納確認

show ipsec profileコマンドにて、IPsecプロファイルに設定したpeerのFQDNが、DNSによって名前解決され、IPアドレスが登録されていることを確認します。

```
WA1020(config)# show ipsec profile [Enter]
ipsec-profile-name: ipsecprof1
  encapsulation mode: tunnel
  source: -
  peer[MUST]: wa2*********.waddns.com
          -> 192.0.2.2
  ike policy[MUST]: ikepol1
  ipsec policy[MUST]: ipsecpol1
WA1020(config)#
```

注意　PeerのFQDNアドレスについて、IPアドレス解決が行われるのは、SAが切れた場合、peerコマンドで登録した場合、未解決のIPアドレスからIKEの接続が合った場合です。古いアドレスが登録されている場合は、項目3の装置BのDynamic DNSの登録が行われているか、再度確認を実施し、取得したIPアドレスの更新を確認してください。

以下、上記で説明した装置A、装置Bの設定について、peer FQDN設定を中心に示します。

装置 A

```
!
hostname WA1020
!
!
no wireless-adapter enable
!
interface FastEthernet0.0
  ip address 192.168.1.200/24
  no shutdown
!
interface FastEthernet1.0
  ip address dhcp
  auto-connect
  ip napt enable
  ip napt reserve esp
  ip napt reserve udp 500
  no shutdown
!
!
interface IPsec0
  ip address unnumbered
  ip tcp adjust-mss auto
  ipsec map ipsecprof1
  no shutdown
!
!
ip route 192.168.10.0/24 IPsec0
ip route default FastEthernet1.0
!
proxy-dns enable
proxy-dns server default FastEthernet1.0 dhcp
!
ike proposal ikeprop1
  encryption-algorithm aes256-cbc
  authentication-algorithm hmac-sha1
  lifetime 28800
  dh-group 1024-bit
!
!
ike policy ikepol1
  mode main
  dpd-keepalive enable 20 3
  proposal ikeprop1
  pre-shared-key plain hogehoge
!
!
ipsec proposal ipsecprop1
  protocol esp enc-algo aes256-cbc auth-algo hmac-sha1-96
  lifetime 28800
!
ipsec policy ipsecpol1
  proposal ipsecprop1
!
ipsec profile ipsecprof1
  mode tunnel
  ipsec policy ipsecpol1
  ike policy ikepol1
  peer wa2*********.waddns.com
!
!
ddns enable
ddns account waddns source-ip auto
!
```

装置 B

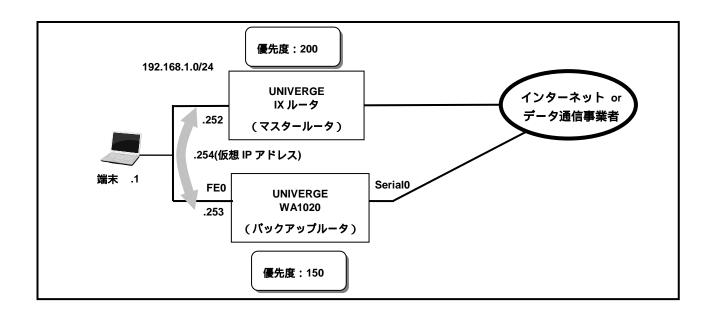
```
!
hostname WA2021
!
!
ppp profile test
  authentication username test
  authentication password plain test
!
interface GigaEthernet0.0
  no ip address
  encapsulation PPPoE0
  no shutdown
!
interface GigaEthernet1.0
  ip address 192.168.10.200/24
  no shutdown
!
interface PPPoE0
  ip address ipcp
  ppp profile test
  auto-connect
  ip napt enable
  ip napt reserve esp
  ip napt reserve udp 500
  no shutdown
!
interface IPsec0
  ip address unnumbered
  ip tcp adjust-mss auto
  ipsec map ipsecprof1
  no shutdown
!
!
ip route default PPPoE0
ip route 192.168.1.0/24 IPsec0
!
proxy-dns enable
proxy-dns server default PPPoE0 ipcp
!
ike proposal ikeprop1
  encryption-algorithm aes256-cbc
  authentication-algorithm hmac-sha1
  lifetime 28800
  dh-group 1024-bit
!
ike policy ikepol1
  mode main
  dpd-keepalive enable 20 3
  proposal ikeprop1
  pre-shared-key plain hogehoge
!
!
ipsec proposal ipsecprop1
  protocol esp enc-algo aes256-cbc auth-algo hmac-sha1-96
  lifetime 28800
!
ipsec policy ipsecpol1
  proposal ipsecprop1
!
ipsec profile ipsecprof1
  mode tunnel
  ipsec policy ipsecpol1
  ike policy ikepol1
  peer wa1*********.waddns.com
!
!
ddns enable
ddns account waddns source-ip auto
!
!
```

VRRP設定例

VRRPを使用した機器冗長の基本的な設定を説明します。本設定により複数の機器を用いた機器冗長が可能になります。各コマンドの詳細については、コマンドリファレンスをご参照ください。

ルータの基本的な通信設定は、完了している状態からの説明とします。

以下の手順にて設定を行います。

1） VRRPグループIDと仮想IPアドレスの設定
2） 優先度の設定
3） 広告パケット送信間隔の設定
4） VRRPの有効設定

WA1020を利用し、UNIVERGE IXルータと機器冗長する場合の例です。

メモ　VRRP グループ ID、仮想 IP アドレス、及び広告パケット送信間隔は、IX ルータ/WA1020 共に同じ値を設定してください。

メモ　LAN 上に接続する端末のデフォルトゲートウェイは、仮想 IP アドレスに設定してください。

メモ　優先度は値の大きい方が優先されるため、IX ルータを 200、WA1020 を 150 とします。

1） VRRPグループIDと仮想IPアドレスの設定

VRRPでは、同じグループID内で冗長管理を行います。以下では、グループIDを1として、VRRP上で制御する仮想IPアドレスを設定します。

```
WA1020(config)# interface FastEthernet0.0 [Enter]
WA1020(config-FastEthernet0.0)# vrrp 1 ip 192.168.1.254 [Enter]
```

2） 優先度の設定

マスター/バックアップ動作を行うための優先度の設定を行います。

```
WA1020(config-FastEthernet0.0)# vrrp 1 priority 150 [Enter]
```

3） 広告パケット送信間隔の設定

同じVRRPグループIDをもつ機器に対して、自身の設定状態を通知する間隔を設定します。送信間隔は秒単位で設定します。

```
WA1020(config-FastEthernet0.0)# vrrp 1 timers advertisement 5 [Enter]
WA1020(config-FastEthernet0.0)# exit [Enter]
```

4） VRRPの有効設定

VRRP機能を有効にします。

```
WA1020(config)# vrrp enable [Enter]
```

以下、上記で説明したWA1020の設定を中心に示します。

```
hostname WA1020
!
no wireless-adapter enable
!
ppp profile test
  authentication username test
  authentication password plain test
!
interface FastEthernet0.0
  ip address 192.168.1.253/24
  vrrp 1 ip 192.168.1.254
  vrrp 1 priority 150
  vrrp 1 timers advertisement 5
  no shutdown
!
interface Serial0
  ip address ipcp
  ppp profile test
  ip napt enable
  mobile id PPP 1 net.example.com
  mobile number *99***CID#
  auto-connect
  no shutdown
!
ip route default Serial0
!
proxy-dns enable
proxy-dns server default Serial0 ipcp
!
vrrp enable
!
```

無線LAN設定例

無線LAN機能はWA2021のみ対応しております。

無線LANを使用した設定を説明します。本設定によりWA2021を無線LANアクセスポイントとして使用することが可能となります。WA2021では、最大4個のアクセスポイントを設定することが可能です。

以下では、WA2021のGigaEthernet1.0インタフェースと無線LANインタフェースWirelessEthernet0.0をブリッジ接続しインタネットアクセスする設定例を示します。

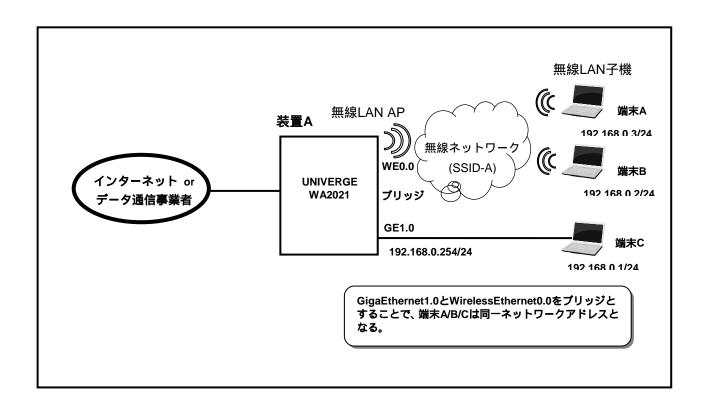
各コマンドの詳細については、コマンドリファレンスをご参照ください。ルータのWAN側の設定やデフォルトルートの通信設定は、完了している状態からの説明とします。

以下の手順にて設定を行います。

1）SSID(ネットワーク名)の設定

2）無線通信モードの設定

3）暗号化の設定

4）ブリッジの設定

1）SSID(ネットワーク名)の設定

子機側が無線LAN-APを識別するためのSSID(ネットワーク名)を設定します。

```
WA2021(config)# interface WirelessEthernet0.0 [Enter]
WA2021(config-WirelessEthernet0.0)# ssid SSID-A [Enter]
WA2021(config-WirelessEthernet0.0)# exit [Enter]
WA2021(config)#
```

2）無線通信モードの設定

無線 LAN の通信モードを設定します。

```
WA2021(config)# interface WirelessEthernet0.0 [Enter]
WA2021(config-WirelessEthernet0.0)# ieee80211 bgn single auto [Enter]
WA2021(config-WirelessEthernet0.0)# exit [Enter]
WA2021(config)#
```

3）暗号化の設定

無線 LAN の暗号化モード、および暗号化キーを設定します。これらの設定は子機にも設定する必要があります。

```
WA2021(config)# interface WirelessEthernet0.0 [Enter]
WA2021(config-WirelessEthernet0.0)# encryption mode wpa-wpa2-psk aes-tkip [Enter]
WA2021(config-WirelessEthernet0.0)# encryption wpa-key aabbccddeeffg [Enter]
WA2021(config-WirelessEthernet0.0)# exit [Enter]
WA2021(config)#
```

4）ブリッジの設定

LAN インタフェース(GigaEthernet1.0)とブリッジさせることで、無線 LAN 接続子機を同一ネットワークに属するように設定します。

```
WA2021(config)# bridge ieee enable
WA2021(config)# interface WirelessEthernet0.0 [Enter]
WA2021(config-WirelessEthernet0.0)# bridge ieee 1 [Enter]
WA2021(config-WirelessEthernet0.0)# exit [Enter]
WA2021(config)# interface GigaEthernet1.0 [Enter]
WA2021(config-GigaEthernet1.0)# bridge ieee 1 [Enter]
WA2021(config-GigaEthernet1.0)# exit [Enter]
WA2021(config)#
```

以下、上記で説明した無線 LAN の設定を示します。

装置 A

```
hostname WA2021
!
Bridge ieee enable
!
interface GigaEthernet1.0
  ip address 192.168.0.254/24
  bridge ieee 1
  no shutdown
!
interface WirelessEthernet0.0
  ssid SSID-A
  encryption mode wpa-wpa2-psk aes-tkip
  encryption wpa-key aabbccddeeffg
  no ip address
  bridge ieee 1
  no shutdown
!
```

6

管理と保守

USBストレージ機能

本製品に接続したオプション品のUSBメモリがUSBストレージとして動作し、フラッシュメモリとの間でプログラムファイルやコンフィグレーションファイルをコピーすることや、TFTP／FTPクライアント機能を使用して、TFTP／FTPサーバにファイル転送することができます。本USBストレージには、以下のような機能もあります。

- syslogのバックアップをUSBメモリに保存できます。
- 障害時等の情報収集を行うテクニカルサポート情報の保存ができます。
- 初期状態の本製品に運用で使用するプログラムファイル、スタートアップコンフィグを保存したUSBメモリを接続して運用設定へ自動更新することができます。

USBストレージのそれぞれの手順等は、本章「ソフトウェアバージョンアップ」、「ファイル転送」、「イベント情報の収集の設定」の項目で説明しています。

本項では、テクニカルサポート情報の保存について説明します。

■テクニカルサポート情報を USB ストレージへ保存

copyコマンドを使用して、テクニカルサポート情報(show technical-support)情報を画面に表示せず、USBストレージへ直接出力して保存します。ファイル名省略することで、取得時の装置時間がファイル名に付加されます。

● USBストレージへのファイル出力

```
WA1500# copy technical-support usb-storage
Save to tech_support_20140308_022008.txt
WA1500#
```

注意　USBストレージ機能で使用できるUSBメモリは、オプション品のみとなります。市販のUSBメモリは使用できません。

メモ　USBストレージ機能は、ソフトウェアバージョン 5.1から対応しています。

ソフトウェアバージョンアップ

■プログラムファイルのバージョンアップ

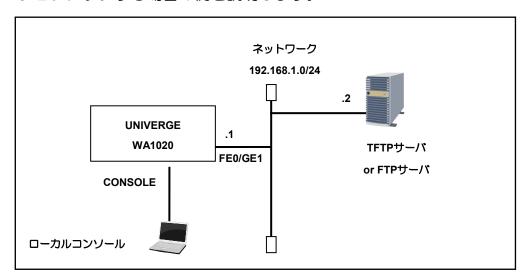
ソフトウェアのバージョンアップは、本製品のTFTP及びFTPクライアント機能を使用して、新しいプログラムファイルをTFTP/FTPサーバからネットワーク経由でダウンロードすることで行います。また、ソフトウェアバージョン 5.1以降は、USBストレージから、ダウンロードすることができます。

メモ　本製品にアクセスするコンソールは、ローカルコンソールまたはリモートコンソールのどちらでもかまいません。

メモ　FTPクライアントはソフトウェアバージョン 2.2から対応しています。

注意　バージョンアップ中は絶対に本製品の電源をOFFにしないでください。製品のフラッシュメモリが破損し、製品が起動しなくなる場合があります。

注意　WA1020用のプログラムファイル名は「WA1020_*_*_*.bin」で、WA2020用は「WA2020_*_*_*.bin」、WA2021用は「WA2021_*_*_*.bin」となります。誤ったファイル名を指定するとダウンロードできませんので注意願います。

以下のネットワーク構成において、プログラムファイルのバージョンを 3.1.4 から 5.1.2 へバージョンアップする場合の例を説明します。

バージョンアップは次の手順で行います。

① バージョンとレビジョンの確認
② プログラムファイルのダウンロード
③ ダウンロードしたプログラムファイルの確認
④ 起動プログラムファイルの指定
⑤ 再起動
⑥ バージョンアップ結果の確認

①バージョンとレビジョンの確認

前準備として、本製品とTFTPサーバ間の接続に問題ないか ping を使って確認してください。また、show versionコマンドを使って現在のプログラムファイルのバージョンと製品レビジョンを確認します。以下の例では、プログラムファイルのバージョンが 3.1.4 に、製品レビジョンが2.0になっています。

```
WA1020(config)# show version [Enter]
Copyright (c) NEC Platforms, Ltd. 2009-2010 All rights reserved.
Copyright (c) 1996-2004
   The NetBSD Foundation, Inc.  All rights reserved.
Copyright (c) 1982, 1986, 1989, 1991, 1993
   The Regents of the University of California.  All rights reserved.
Operating System Software : version 3.1.4
Compiled:  Thu Nov 18 10:27:43 JST 2010

Serial Number: 11*******

Hardware Revision:2.0
uptime is 0 days 0 hours 8 minutes 39 secs.
memory size is 134217728 [byte]
WA1020(config)#
```

プログラムファイルのバージョンを確認します。

製品レビジョンが表示されます。

注意　製品レビジョンは、プログラムファイルのバージョンが2.1以降でないと表示されません。製品レビジョンが表示されない場合の製品レビジョンは、1.0です。

②プログラムファイルのダウンロード

TFTP の場合

tftp get コマンドを使用して、TFTPサーバからプログラムファイルのダウンロードを行います。ダウンロード中は、「#」にて進行状況を確認することができます。

```
WA1020# tftp get 192.168.1.2:wa1020_5_1_2.bin wa1020_5_1_2.bin [Enter]
connect to
192.168.1.2 ...#################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
##################
Verify Firmware ...
Update Firmware ...
Write verify Firmware ...
WA1020#
```

メモ　なんらかの理由により、プログラムファイルのダウンロードに失敗すると「 % Invalid Firmware」が表示されます。

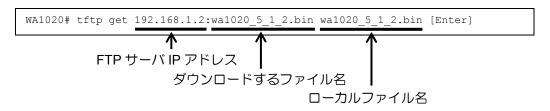
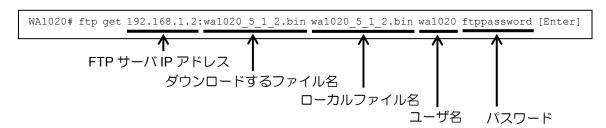
```
WA1020# tftp get 192.168.1.2:wa1020_5_1_2.bin wa1020_5_1_2.bin [Enter]
connect to 192.168.1.2 ...##############################################
############################################################################
############################################################################
############################################################################
#############
Verify Firmware ...
% Invalid Firmware
WA1020#
```

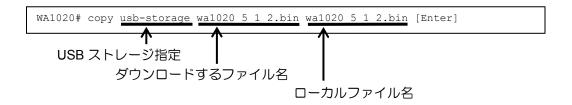
FTP の場合

ftp get コマンドを使用して、FTPサーバからプログラムファイルのダウンロードを行います。例では、username wa1020 password ftppasswordのアカウントで実施しています。anonymousも指定可能です。ダウンロード中は、「#」にて進行状況を確認することができます。

```
WA1020# ftp get 192.168.1.2:wa1020_5_1_2.bin wa1020_5_1_2.bin wa1020 ftppassword [Enter]
connect to 192.168.1.2 ... ##################################################
Verify Firmware ...
Update Firmware ...
Write verify Firmware ...
WA1020#
```

メモ　なんらかの理由により、プログラムファイルのダウンロードに失敗すると「 % Invalid Firmware」が表示されます。

```
WA1020# ftp get 192.168.1.2:wa1020_5_1_2.bin wa1020_5_1_2.bin [Enter]
connect to 192.168.1.2 ... ##############################################
Verify Firmware ...
% Invalid Firmware
WA1020#
```

USB ストレージの場合　(ver5.1:追加パラメータ)

copyコマンドを使用して、USBストレージ上の指定したプログラムファイルをダウンロードします。(本パラメータは、ソフトウェアバージョン5.1以降で使用できます。)

以下の例では、プログラムファイルを上書きでダウンロードしています。

```
WA1020# copy usb-storage wa1020_5_1_2.bin wa1020_5_1_2.bin [Enter]
Copying from "wa1020_5_1_2.bin" to "wa1020_5_1_2.bin"
Are you sure you want to overwrite? (Yes or no) y
Copy succeeded
WA1020#
```

③ダウンロードしたプログラムファイルの確認

show storage コマンドを使用してファイル名とファイルサイズを確認し、プログラムファイルが正常にダウンロードできたことを確認します。

```
WA1020# show storage [Enter]
wa1020_5_1_2.bin          6371704 bytes
wa1020_3_1_4.bin    5147312 bytes
startup.conf        669 bytes
WA1020#
```

④起動プログラムファイルの指定

boot entry コマンドにてプログラムファイルを指定する方法と、不要なプログラムファイルを削除してプログラムファイルを1つにして起動する方法があります。

boot entry コマンドにてプログラムファイルを指定する場合、boot entry コマンドにて設定を行い、saveコマンドにより設定を保存します。

```
WA1020(config)# boot entry flash wa1020_5_1_2.bin [Enter]
WA1020(config)# save [Enter]
WA1020(config)#
```

不要なプログラムファイルを削除してプログラムファイルを1つにして起動する場合、erase firmwareコマンドにてプログラムファイルを指定して削除します。

```
WA1020(config)# erase firmware wa1020_3_1_4.bin [Enter]
WA1020(config)#
```

メモ　boot entry コマンドを設定しない場合で、かつ複数のプログラムファイルが存在する場合、show storage コマンド実行結果の最初に表示されるプログラムファイルが起動時に読み込まれます。

⑤再起動

rebootコマンドを使用して、プログラムファイルの再読み込みを行います。

```
WA1020# reboot [Enter]
Are you sure you want to reboot the router? (Yes or No): y [Enter]
```

rebootコマンドを実行すると、起動の様子がコンソール画面に表示されます。起動ファイルが正しいか確認してください。また、ログインプロンプトが表示されるまで、そのままお待ちください。

```
WA1020# reboot [Enter]
Are you sure you want to reboot the router? (Yes or No): y
# reboot....

IPL: SOFT-RESET
IPL: MEMORY OK

Boot: Version 2.1.0
POST:
DRAM Test ..... PASS
TClock Test ... PASS
FLASH CHKSUM .. PASS
LAN Test ..... PASS
PCI Test ..... PASS
USB Test .... PASS
3DES->HMAC-SHA1 TEST ... PASS
AES256->HMAC-SHA1 TEST ... PASS
DES->HMAC-MD5 TEST ... PASS
3DES->HMAC-MD5 TEST ... PASS
AES128->HMAC-MD5 TEST ... PASS
AES192->HMAC-MD5 TEST ... PASS
AES256->HMAC-MD5 TEST ... PASS
NULL->HMAC-MD5 TEST ... PASS
post success
LM: loading "wa1020_5_1_2.bin"
..............................................................................
...
Sat Jan 10 04:03:16 JST 2009

WA1020 console

login:
```

メモ　telnetを使用中に reboot コマンドを実行した場合、telnetセッションが切断されますので、起動メッセージは表示されませんので、30秒程度待ってから再接続を行い、次の手順に進んでください。

注意　rebootコマンドを実行してから、ログインプロンプトが表示されるまで、絶対に本製品の電源をOFFにしないでください。本製品のフラッシュメモリが破損し、製品が立ち上がらなくなる場合があります。

⑥バージョンアップ結果の確認

show version コマンドを使って、バージョアップが完了していることを確認します。
以下の例では、プログラムファイルのバージョンが 5.1.2 になっています。

```
WA1020# show version[Enter]
Copyright (c) NEC Platforms, Ltd. 2009-2014 All rights reserved.
Copyright (c) 1996-2004
   The NetBSD Foundation, Inc.  All rights reserved.
Copyright (c) 1982, 1986, 1989, 1991, 1993
   The Regents of the University of California.  All rights reserved.
Operating System Software : version 5.1.2
Compiled:  Thu Apr 10 16:43:12 JST 2014
Serial Number: 09*******

Hardware Revision: 2.0
uptime is 0 days 0 hours 2 minutes 25 secs.
memory size is 134217728 [byte]
WA1020#
```

プログラムファイルのバージョンを確認します。

■ブートファイルのバージョンアップ

ブートファイルのバージョンアップについて説明します。

プログラムファイルをバージョンアップする際に、バージョンアップするプログラムファイルの版数によっては、ブートファイルを指定の版数に合わせることが必要な場合があります。

ブートファイルのバージョンアップ措置が必要となる場合は、以下です。

対象装置　　　　　　　　　　　　：WA2020

使用中のソフトウェアバージョン：4.1以前

更新後のソフトウェアバージョン：4.2以降

ブートファイルのバージョンは、ローカルコンソールを接続した状態で再起動を実施し、起動時のコンソールメッセージに表示されるバージョンをご確認ください。

ブートファイルのバージョンアップは、ブートバージョンアップ専用プログラムファイルで装置を起動することによりブートファイルのバージョンアップ処理が実行されます。

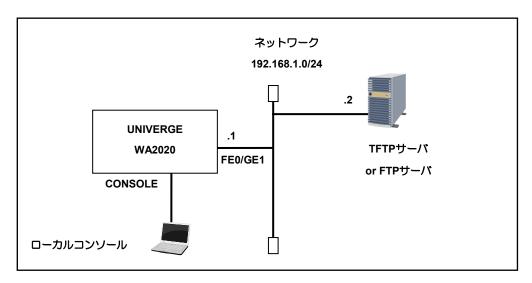
注意　ブートファイル更新のため、本製品にアクセスするコンソールは、ローカルコンソールでの使用をお願いします。

注意　バージョンアップ中は絶対に本製品の電源をOFFにしないでください。製品のフラッシュメモリが破損し、製品が起動しなくなる場合があります。

注意　ブートバージョンアップ専用プログラムファイルは、ブートファイル書き換え専用です。そのまま通常の運用には使用できません。必ずリリースされているプログラムファイルに入れ替えてご利用ねがいます。

注意　WA1020用のブートバージョンアップ専用プログラムファイル名は「WA1020_*_*_*boot.bin」で、WA2020用は「WA2020_*_*_*boot.bin」、WA2021用は「WA2021_*_*_*boot.bin」となります。誤ったファイル名を指定するとダウンロードできませんので注意願います。

メモ　FTPクライアントはソフトウェアバージョン 2.2から対応しています。

以下のネットワーク構成において、WA2020のブートファイルのバージョンを 1.0.0 から 1.0.1 へバージョンアップする場合の例を説明します。

バージョンアップは次の手順で行います。

ブートファイルバージョンとプログラムファイルの確認
① ブートバージョンアップ専用プログラムファイルのダウンロード
② ダウンロードしたプログラムファイルの確認
③ プログラムファイル削除
④ 再起動
⑤ ブートファイルバージョンアップ結果の確認
⑥ 再起動時のブートバージョン確認
⑦ 利用するプログラムファイルのダウンロード
⑧ ダウンロードしたプログラムファイルの確認
⑨ ブートバージョンアップ専用プログラムファイル削除
⑩ 削除したプログラムファイルの確認
⑪ 再起動
⑫ プログラムファイルのバージョン確認

①ブートファイルバージョンとプログラムファイルの確認

前準備として、本製品とTFTPサーバ間の接続に問題ないか ping を使って確認してください。

再起動を実施して、起動時のコンソール表示から現在のブートファイルのバージョンを確認します。

```
IPL: SOFT-RESET
IPL: MEMORY OK
IPL: LOADING BOOT

Boot: Version 1.0.0
POST:
DRAM Test ..... PASS
TClock Test ... PASS
RTC Test ...... PASS
FLASH CHKSUM .. PASS
WAN Test ..... PASS
LAN Test ..... PASS
PCI Test ..... PASS
3DES->HMAC-SHA1 TEST ... PASS
AES256->HMAC-SHA1 TEST ... PASS
DES->HMAC-MD5 TEST ... PASS
3DES->HMAC-MD5 TEST ... PASS
AES128->HMAC-MD5 TEST ... PASS
AES192->HMAC-MD5 TEST ... PASS
AES256->HMAC-MD5 TEST ... PASS
NULL->HMAC-MD5 TEST ... PASS
USB Test .... PASS
post success
LM: loading "wa2020_4_0_1.bin"
..........................................................................
.................
Thu Feb  9 18:59:44 JST 2012

WA2020 console

login:
```

ブートファイルのバージョンが表示されます。

②ブートバージョンアップ専用プログラムファイルのダウンロード

以下の例では、ブートバージョンアップ専用プログラムファイルのバージョンが 4.2.3b の場合を示します。

TFTP の場合

tftp get コマンドを使用して、TFTPサーバからプログラムファイルのダウンロードを行います。ダウンロード中は、「#」にて進行状況を確認することができます。

```
WA2020# tftp get 192.168.1.2:wa2020_4_2_3boot.bin wa2020_4_2_3boot.bin [Enter]
connect to
192.168.1.2 ...##############################################################
#############################################################################
#############################################################################
#############################################################################
#############################################################################
#############################################################################
#############################################################################
#############################################################################
#############################################################################
#############################################################################
#############################################################################
#############################################################################
#############################################################################
##################
Verify Firmware ...
Update Firmware ...
Write verify Firmware ...
WA2020#
```

メモ　なんらかの理由により、プログラムファイルのダウンロードに失敗すると「 % Invalid Firmware」が表示されます。

```
WA2020# tftp get 192.168.1.2:wa2020_4_2_3boot.bin wa2020_4_2_3boot.bin [Enter]
connect to
192.168.1.2 ...#################################################################
################################################################################
################################################################################
##############################################################################
Verify Firmware ...
% Invalid Firmware
WA2020#
```

FTP の場合

ftp get コマンドを使用して、FTPサーバからプログラムファイルのダウンロードを

行います。例では、username wa1020 password ftppasswordのアカウントで実施しています。anonymousも指定可能です。ダウンロード中は、「#」にて進行状況を確認することができます。

```
WA2020# ftp get 192.168.1.2:wa2020_4_2_3boot.bin wa2020_4_2_3boot.bin wa1020
ftppassword [Enter]
connect to 192.168.1.2 ... ##################################################
Verify Firmware ...
Update Firmware ...
Write verify Firmware ...
WA2020#
```

メモ　なんらかの理由により、プログラムファイルのダウンロードに失敗すると「 % Invalid Firmware」が表示されます。

```
WA2020# ftp get 192.168.1.2:wa2020_4_2_3boot.bin wa2020_4_2_3boot.bin [Enter]
connect to 192.168.1.2 ... ##############################################
Verify Firmware ...
% Invalid Firmware
WA2020#
```

③ダウンロードしたプログラムファイルの確認

show storage コマンドを使用してファイル名とファイルサイズを確認し、プログラムファイルが正常にダウンロードできたことを確認します。

```
WA2020# show storage [Enter]
wa2020_4_0_1.bin     5305668 bytes
wa2020_4_2_3boot.bin     5630816 bytes
startup.conf        456 bytes

total 16515072 bytes, avail 5371328 bytes
WA2020#
```

④プログラムファイル削除

ブートバージョンアップ専用プログラムファイルを起動するため、不要なプログラムファイルを削除してプログラムファイルを1つにして起動します。

erase firmwareコマンドにてプログラムファイルを指定して削除します。

```
WA2020(config)# erase firmware wa2020_4_0_1.bin [Enter]
WA2020(config)# 
```

メモ　boot entry コマンドを使用してブートバージョンアップ専用プログラムファイルを設定することも可能ですが、再起動時にブートバージョンアップ専用プログラムファイルが起動していることを確認してください。間違えるとブートファイルが書き変わりません。また、ブートファイルが書き変わった後、すみやかにboot entry コマンドを削除するか、利用するプログラムファイル指定に書き換えてください。再起動のたびにブートファイルの書き直しが繰り返されます。

⑤再起動

rebootコマンドを使用して、ブートバージョンアップ専用プログラムファイルの読み込みを行います。

```
WA2020# reboot [Enter]
Are you sure you want to reboot the router? (Yes or No): y [Enter]
```

rebootコマンドを実行すると、起動の様子がコンソール画面に表示されます。起動ファイルが正しいか確認してください。ログインプロンプトが表示される前にブートファイルの書き換えが実行され、メッセージが表示されます。ログインプロンプトが表示されるまで、そのままお待ちください。

```
WA2020# reboot[Enter]
Are you sure you want to reboot the router? (Yes or No): y
# reboot....

IPL: SOFT-RESET
IPL: MEMORY OK
IPL: LOADING BOOT

Boot: Version 1.0.0
POST:
DRAM Test ..... PASS
TClock Test ... PASS
RTC Test ...... PASS
FLASH CHKSUM .. PASS
WAN Test ..... PASS
LAN Test ..... PASS
PCI Test ..... PASS
3DES->HMAC-SHA1 TEST ... PASS
AES256->HMAC-SHA1 TEST ... PASS
DES->HMAC-MD5 TEST ... PASS
3DES->HMAC-MD5 TEST ... PASS
AES128->HMAC-MD5 TEST ... PASS
AES192->HMAC-MD5 TEST ... PASS
AES256->HMAC-MD5 TEST ... PASS
NULL->HMAC-MD5 TEST ... PASS
USB Test .... PASS
post success
LM: loading "wa2020_4_2_3boot.bin"   ← ブートファイルが更新されます。
.........................................................................
.................
Update bootstrap...Complete.
Mon Mar 19 14:41:13 JST 2012

WA2020 console

       _
```

rebootコマンドを実行してから、ログインプロンプトが表示されるまで、絶対に本製品の電源をOFFにしないでください。本製品のフラッシュメモリが破損し、製品が立ち上がらなくなる場合があります。

⑥ブートファイルバージョンアップ結果の確認

show version コマンドを使って、ブートバージョンアップ専用プログラムで起動していることを確認します。

以下の例では、ブートバージョンアップ専用プログラムファイルのバージョンが 4.2.3b になっていることを確認します。ブートバージョンアップ専用プログラムファイルは、バージョンの末尾に「b」がつきます。

```
WA2020# show version[Enter]
Copyright (c) NEC Platforms, Ltd. 2011-2012 All rights reserved.
Copyright (c) 1996-2004
   The NetBSD Foundation, Inc.  All rights reserved.
Copyright (c) 1982, 1986, 1989, 1991, 1993
   The Regents of the University of California.  All rights reserved.
Operating System Software : version 4.2.3b
Compiled:  Fri Mar 16 15:08:50 JST 2012

Serial Number: 11*******

uptime is 0 days 0 hours 0 minutes 20 secs.
memory size is 134217728 [byte]
WA2020#
```

ブートバージョンアップ専用プログラムファイルのバージョンを確認します。

⑦再起動時のブートバージョン確認

rebootコマンドを使用して、再度ブートバージョンアップ専用プログラムファイルの読み込みを行います。

```
WA2020# reboot [Enter]
Are you sure you want to reboot the router? (Yes or No): y [Enter]
```

rebootコマンドを実行すると、起動の様子がコンソール画面に表示されます。ブートファイルが更新されたか確認してください。ログインプロンプトが表示されるまで、そのままお待ちください。

```
WA2020# reboot[Enter]
Are you sure you want to reboot the router? (Yes or No): y
# reboot....

IPL: SOFT-RESET
IPL: MEMORY OK
IPL: LOADING BOOT

Boot: Version 1.0.1
POST:
DRAM Test ..... PASS
TClock Test ... PASS
RTC Test ...... PASS
FLASH CHKSUM .. PASS
WAN Test ..... PASS
LAN Test ..... PASS
PCI Test ..... PASS
3DES->HMAC-SHA1 TEST ... PASS
AES256->HMAC-SHA1 TEST ... PASS
DES->HMAC-MD5 TEST ... PASS
3DES->HMAC-MD5 TEST ... PASS
AES128->HMAC-MD5 TEST ... PASS
AES192->HMAC-MD5 TEST ... PASS
AES256->HMAC-MD5 TEST ... PASS
NULL->HMAC-MD5 TEST ... PASS
USB Test .... PASS
post success
LM: loading "wa2020_4_2_3boot.bin"
.........................................................................
.................
Update bootstrap...Complete.
Mon Mar 19 14:51:13 JST 2012

WA2020 console

login:
```

更新されたブートファイルのバージョンが表示されます。

注意　rebootコマンドを実行してから、ログインプロンプトが表示されるまで、絶対に本製品の電源をOFFにしないでください。本製品のフラッシュメモリが破損し、製品が立ち上がらなくなる場合があります。

⑧利用するプログラムファイルのダウンロード

②項と同様にtftp/ftp get コマンドを使用して、プログラムファイルのダウンロードを行います。作業イメージは、②を参照ねがいます。

⑨ダウンロードしたプログラムファイルの確認

show storage コマンドを使用してファイル名とファイルサイズを確認し、プログラムファイルが正常にダウンロードできたことを確認します。

```
WA2020# show storage [Enter]
wa2020_4_2_3.bin     5532856 bytes
wa2020_4_2_3boot.bin     5630816 bytes
startup.conf        456 bytes

total 16515072 bytes, avail 5109312 bytes
WA2020#
```

⑩ブートバージョンアップ専用プログラムファイル削除

ブートバージョンアップ専用プログラムファイルを削除して、利用するプログラムファイル1つにして起動します。

erase firmwareコマンドにてプログラムファイルを指定して削除します。

```
WA2020(config)# erase firmware wa2020_4_2_3boot.bin [Enter]
WA2020(config)#
```

注意　必ずブートバージョンアップ専用プログラムファイルは削除してください。このプログラムファイルでは、運用ソフトウェアとして使用できません。

⑪削除したプログラムファイルの確認

show storage コマンドを使用して、ブートバージョンアップ専用プログラムファイルが削除できたことを確認します。

```
WA2020# show storage [Enter]
wa2020_4_2_3.bin     5532856 bytes
startup.conf        456 bytes

total 16515072 bytes, avail 10742656 bytes
WA2020#
```

⑫再起動

rebootコマンドを使用して、プログラムファイルの再読み込みを行います。

```
WA2020# reboot [Enter]
Are you sure you want to reboot the router? (Yes or No): y [Enter]
```

rebootコマンドを実行すると、起動の様子がコンソール画面に表示されます。起動ファイルが正しいか確認してください。また、ログインプロンプトが表示されるまで、そのままお待ちください。

```
WA2020# reboot [Enter]
Are you sure you want to reboot the router? (Yes or No): y
# reboot....

IPL: SOFT-RESET
IPL: MEMORY OK
IPL: LOADING BOOT

Boot: Version 1.0.1
POST:
DRAM Test ..... PASS
TClock Test ... PASS
RTC Test ...... PASS
FLASH CHKSUM .. PASS
WAN Test ..... PASS
LAN Test ..... PASS
PCI Test ..... PASS
3DES->HMAC-SHA1 TEST ... PASS
AES256->HMAC-SHA1 TEST ... PASS
DES->HMAC-MD5 TEST ... PASS
3DES->HMAC-MD5 TEST ... PASS
AES128->HMAC-MD5 TEST ... PASS
AES192->HMAC-MD5 TEST ... PASS
AES256->HMAC-MD5 TEST ... PASS
NULL->HMAC-MD5 TEST ... PASS
USB Test .... PASS
post success
LM: loading "wa2020 4 2 3.bin"
........................................................................
.................
Mon Mar 19 14:55:27 JST 2012

WA2020 console

login:
```

起動ファイル名を確認します。

注意　rebootコマンドを実行してから、ログインプロンプトが表示されるまで、絶対に本製品の電源をOFFにしないでください。本製品のフラッシュメモリが破損し、製品が立ち上がらなくなる場合があります。

⑬プログラムファイルのバージョン確認

show version コマンドを使って、ブートバージョンアップ専用プログラムファイルではなく、利用するプログラムファイルが起動し、バージョアップが完了していることを確認します。以下の例では、プログラムファイルのバージョンが 4.2.3 になっています。

```
WA2020# show version[Enter]
Copyright (c) NEC Platforms, Ltd. 2011-2012 All rights reserved.
Copyright (c) 1996-2004
   The NetBSD Foundation, Inc.  All rights reserved.
Copyright (c) 1982, 1986, 1989, 1991, 1993
   The Regents of the University of California.  All rights reserved.
Operating System Software : version 4.2.3
Compiled:  Fri Mar 16 15:21:39 JST 2012

Serial Number: 11*******

uptime is 0 days 0 hours 0 minutes 20 secs.
memory size is 134217728 [byte]
WA2020#
```

プログラムファイルのバージョンを確認します。末尾に b がついていないことを確認ください。

■USBストレージ機能による自動バージョンアップ

USBストレージ機能を使用した、初期状態(工場出荷状態)からのプログラムファイルのバージョンアップ/スタートアップコンフィグファイルの自動設定について説明します。

あらかじめプログラムファイル及びスタートアップコンフィグファイルを保存したUSBメモリを、初期状態の装置に接続することにより、USBメモリ内から自動的にフラッシュメモリへ保存します。

これにより、キッティング作業の作業迅速化等、設置時の複数機器での動作プログラムファイルのバージョン統一化が簡単になります。故障交換時の作業にも利用できます。

USBストレージの本機能を使用するために格納するファイル名は、以下であることが必要です。

スタートアップコンフィグファイル：startup.conf
プログラムファイル：装置名.bin
WA1020用：wa1020.bin
WA1510用：wa1500.bin
WA1511用：wa1500.bin
WA2020用：wa2020.bin
WA2021用：wa2021.bin

注意　初期化状態でのみ動作する機能なので、スタートアップコンフィグファイルが装置内に存在する状態では、動作しません。

注意　USBメモリは、あらかじめ使用するプログラムファイルまたは、スタートアップコンフィグファイル、もしくはその両方が格納されている必要があります。

注意　USBストレージ機能で使用できるUSBメモリは、オプション品のみとなります。市販のUSBメモリは使用できません。

メモ　USBストレージ機能での自動更新は、ソフトウェアバージョン 5.1から対応しています。

WA1510のプログラムファイルのバージョンを変更し、スタートアップコンフィグファイルを登録する場合の例を説明します。

作業は次の手順で行います。

① USBメモリへのプログラムファイル／スタートアップコンフィグファイル格納
② WA1510初期化実施
③ USBメモリ接続→自動更新
④ 起動ソフトウェアバージョンとコンフィグの確認　(コンソールがある場合)

①USB メモリへのプログラムファイル／スタートアップコンフィグファイル格納

前準備として、オプション品のUSBメモリにプログラムファイル／スタートアップコンフィグファイルを格納します。ファイル名は上記で示されている「wa1500.bin」、「startup.conf」で格納します。

②WA1510 初期化実施

工場出荷ではない場合、WA1510を初期化起動します。背面の初期化(init)ボタンを押下しながら、電源をON します。そのまま、ボタンを押下し続けると、PWR、STAT、PPP、MODEの4つのLEDが同時に3回点滅して、初期化開始をお知らせします。

その後、PWR,とSTATランプが緑点灯となることを確認します。

③USB メモリ接続→自動更新

USBスロットにUSBメモリを接続します。USBメモリ上のファイルをフラッシュメモリに自動コピーします。動作時は、PWRランプが緑点滅し、ファイル書き込み中はSTATランプが赤点滅します。

終了すると自動的に再起動となり、全ランプ点灯で再起動スタートが確認できます。

その後、PWR,とSTATランプが緑点灯となることを確認します。

以上でUSBストレージ機能での自動更新手順は終了です。コンソール用PCがある場合は、以下の操作で、更新の確認ができます。

④起動ソフトウェアバージョンとコンフィグの確認

コンソールにて、loginし、以下のコマンドでプログラムソフトウェアが更新され、スタートアップコンフィグファイルが格納されていることを確認します。

```
WA1500# show storage [Enter]
startup.conf        542 bytes
wa1500.bin          4936040 bytes

total 132775936 bytes, avail 127470784 bytes
WA1500#
```

```
WA1500# show version[Enter]
Copyright (c) NEC Platforms, Ltd. 2014 All rights reserved.
Copyright (c) 1996-2004
   The NetBSD Foundation, Inc.  All rights reserved.
Copyright (c) 1982, 1986, 1989, 1991, 1993
   The Regents of the University of California.  All rights reserved.
Bootstrap Software       : version 1.0.1
Operating System Software : version 5.1.2
Compiled:  Thu Apr 10 17:39:29 JST 2014

Serial Number: **********

Embedded Module:
uptime is 0 days 0 hours 11 minutes 10 secs.
memory size is 134217728 [byte]
WA1500#
```

自動更新

自動更新は、本製品のFTPクライアント機能やHTTP接続を使用して、設定されたスケジュールに従い、自動的に新しいファイルをネットワーク経由でダウンロードする機能です。

自動更新は以下の2つの機能を有しております。

- 自動バージョンアップ

  自動的にプログラムファイルをダウンロードできます。
  定義ファイルを用いる方法と直接プログラムファイルを指定する方法があります。
  定義ファイルを利用することで、不必要なプログラムファイルのダウンロードを防ぎ、モバイルブロードバンド回線の通信料金を抑えることが可能です。

- 自動コンフィグファイル更新

  自動的にコンフィグレーションファイルをダウンロードし、スタートアップコンフィグとして保存します。

自動更新は、設定したサーバ(FTP/HTTP)に対し、スケジュール機能によって指定したタイミングで実行されます。また、ダウンロードしたファイルの適用に必要な再起動を実行することができます。

- 起動時指定

  本製品の起動直後に自動更新を実行します。

- 日時指定（定期実行）

  設定した日時での実行や、日毎／週毎／月毎の定期的な実行が可能です。

- 自動再起動機能

  ファイルを正常にダウンロードした場合、自動的に本製品を再起動することで、ダウンロードしたファイルを本製品に適用することができます。

本機能は、以下のような利用シーンで有効です。

- 大規模ネットワークで、一斉に複数台のWAシリーズのバージョンアップを行う場合
  （自動バージョンアップ、日時指定（定期実行））
- 現地調整作業やキッティング作業を削減したい場合
  （自動コンフィグファイル更新、起動時指定）
- 無線LANのSSIDや暗号化キー等、コンフィグの定期的な更新を行う場合
  （自動コンフィグファイル更新、日時指定（定期実行））

■注意事項

自動更新共通

- 本機能はWeb-GUIから設定することはできません。
- 自動更新が起動していた場合以下のコマンドはご利用頂けません。ftp、tftp、save、erase、copy、reboot、clear syslog flash、clear error-log。自動更新処理完了後、該当コマンドを使用してください。
- 自動更新でのFTPはセキュアプロトコルであるftps/sftpに対応していません。

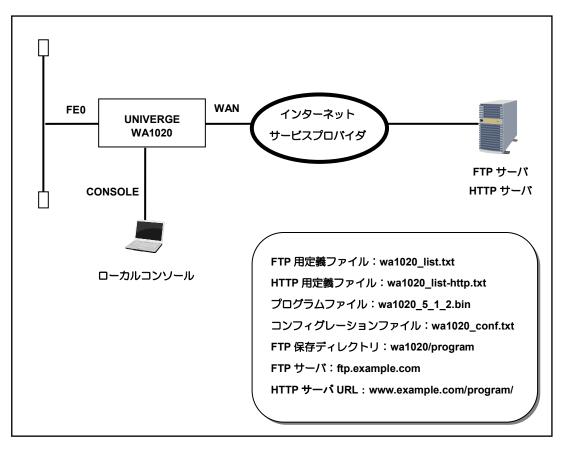
自動バージョンアップ

- FTP自動バージョンアップはソフトウェアバージョン3.2から対応しています。3.2以前のバージョンに変更した場合は、その後本機能は使えなくなります。
  HTTP自動バージョンアップはソフトウェアバージョン5.1から対応しています。5.1以前のバージョンに変更した場合は、その後本機能は使えなくなります。
- 自動バージョンアップでダウンロードされるプログラムファイルは、WA1020の場合は「wa1020.bin」、WA1510、WA1511の場合は「wa1500.bin」、WA2020の場合は「wa2020.bin」、WA2021の場合は「wa2021.bin」という名称でフラッシュメモリに格納されます。
  boot entryコマンドで「wa1020.bin」、「wa1500.bin」、「wa2020.bin」または「wa2021.bin」を指定して下さい。boot entryコマンドを使用しない場合、他のプログラムファイルを削除し、プログラムファイルを「wa1020.bin」、「wa1500.bin」、「wa2020.bin」または「wa2021.bin」のみとしてください。
- 装置内部のフラッシュメモリ容量が足りない場合は自動バージョンアップを実施できません。（同名のファームウェアが存在した場合は上書きします。）不要なプログラムファイルを削除してください。

自動コンフィグファイル更新

- FTP自動コンフィグファイル更新はソフトウェアバージョン4.5から対応しています。4.5以前のバージョンに変更した場合は、その後本機能は使えなくなります。
  HTTP自動コンフィグファイル更新はソフトウェアバージョン5.1から対応しています。5.1以前のバージョンに変更した場合は、その後本機能は使えなくなります。

以下のネットワーク構成において、自動更新を行うための設定例を説明します。

以下では代表例としてWA1020で自動バージョンアップを行う場合と、自動コンフィグファイル更新を行う場合の手順を説明します。

以下の情報を前もって確認しておく必要があります。

■自動バージョンアップ

- WA1020からFTP/HTTPサーバへの通信が可能であること。
- FTP/HTTPサーバに、ダウンロード定義ファイルがあること。
- FTP/HTTPサーバに、定義ファイルで指定したプログラムファイルがあること。
- show storageコマンドにてフラッシュメモリに充分な空き容量があること。

（ソフトウェアバージョン 4.0 以降でのみ本コマンドで空き容量を確認できます）

■自動コンフィグファイル更新

- WA1020からFTP/HTTPサーバへの通信が可能であること。
- FTP/HTTPサーバに、コンフィグレーションファイルがあり、レビジョンコマンドが記載されていること。

■設定手順（自動バージョンアップ）

以下の手順で設定を行います。FTP使用の場合は、①～④を、HTTP使用の場合は、①’～④’を実施します。スケジュール等共通設定は、両サーバとも⑤～⑧を実施します。

なお、コマンドの詳細については、コマンドリファレンスをご参照ください。

FTPサーバの場合

① FTPサーバの設定

② FTPログイン情報の設定

③ FTPモードの設定

④ FTP用定義ファイルの設定

HTTPサーバの場合

①’ HTTPサーバの設定

②’ HTTPログイン情報の設定

③’ HTTP BASIC認証使用/未使用の設定

④’ HTTP用定義ファイルの設定

共通設定

⑤ ダウンロードスケジュールの設定

⑥ 再起動有効設定

⑦ 自動バージョンアップの有効化

⑧ ブートエントリの設定

FTPサーバの場合

①FTPサーバの設定

ダウンロード先のサーバの指定を行います。

```
WA1020(config)# auto-versionup mode ftp [Enter]
WA1020(config)#
```

FTPサーバの設定を行います。ポート番号を初期値の21から変更する場合は、サーバ名の後に設定することができます。

```
WA1020(config)# auto-versionup server ftp.example.com [Enter]
WA1020(config)#
```

②FTPログイン情報の設定

FTPサーバのアカウントパスワードを設定します。例では、以下を設定しています。

アカウント：wa1020

パスワード：ftppassword

```
WA1020(config)# auto-versionup authentication username wa1020[Enter]
WA1020(config)# auto-versionup authentication password plain ftppassword
[Enter]
WA1020(config)#
```

③FTPモードの設定

FTPサーバのモード（Active/Passive）を設定します。FTPモードの初期値はpassiveです。FTPモードを変更しない場合は設定する必要はありません。

```
WA1020(config)# auto-versionup ftpmode passive [Enter]
WA1020(config)#
```

④FTP用定義ファイルの設定

FTP用定義ファイルの設定を行います。

定義ファイルの保存ディレクトリ、および定義ファイルを設定します。

例では、以下を設定しています。

保存ディレクトリ（保存パス）：wa1020/program

定義ファイル　　　　　　　　：wa1020_list.txt

```
WA1020(config)# auto-versionup definition path wa1020/program [Enter]
WA1020(config)# auto-versionup definition filename wa1020_list.txt[Enter]
WA1020(config)#
```

- 定義ファイル(FTPサーバの場合)

定義ファイルとは、ダウンロードできるバージョン、保存ディレクトリ、プログラムファイルを定義したテキストファイルです。

製品は定義ファイルをダウンロードし、バージョン変更の必要があると判断した場合のみ、プログラムファイルのダウンロードを行います。この機能により、不必要な通信を軽減し、無線経由でダウンロードする場合のパケット料金を抑えることができます。

定義ファイルは、半角コロンで区切られたCSVフォーマットを用います。

以下のフォーマットで記載します。

＃ コメント行

「バージョン情報」，「保存ディレクトリ」／「プログラムファイル」

例）

```
# WA1020 最新プログラムファイル
5.1.2,wa1020/program/wa1020_5_1_2.bin
```

● 定義ファイルを指定しない場合

定義ファイルを指定せず、直接ダウンロードするプログラムファイルを指定することができます。プログラムファイルを指定した場合は、バージョン変更の必要がなくても、毎回プログラムファイルのダウンロードを行います。

```
WA1020(config)# auto-versionup firmware path wa1020/program [Enter]
WA1020(config)# auto-versionup firmware filename wa1020_5_1_2.bin [Enter]
WA1020(config)#
```

HTTPサーバの場合

①' HTTPサーバの設定

ダウンロード先のサーバの指定を行います。

```
WA1020(config)# auto-versionup mode http [Enter]
WA1020(config)#
```

②' HTTPログイン情報の設定

HTTPサーバのアカウントパスワードを設定します。BASIC認証のアカウントになります。例では、以下を設定しています。

アカウント：wa1020

パスワード：ftppassword

```
WA1020(config)# auto-versionup authentication username wa1020[Enter]
WA1020(config)# auto-versionup authentication password plain ftppassword
[Enter]
WA1020(config)#
```

③' HTTP BASIC認証使用/未使用の設定

HTTPサーバの場合は、認証の使用有無を設定できます。例では、BASIC認証実施を指定します。

```
WA1020(config)# auto-versionup authentication mode basic [Enter]
WA1020(config)#
```

④' HTTP用定義ファイルの設定

HTTP用定義ファイルの設定を行います。

定義ファイルのURLを設定します。保存パス含めファイル名まで設定します。

例では、以下を設定しています。

URLアドレス（保存パス含）：http://www.example.com/program/wa1020_list-http.txt

定義ファイル　　　　　　　：wa1020_list-http.txt

```
WA1020(config)# auto-versionup definition url http://www.example.com/
program/wa1020_list-http.txt [Enter]
WA1020(config)#
```

● 定義ファイル(HTTPサーバの場合)

定義ファイルとは、ダウンロードできるバージョン、URLにプログラムファイルのパスまで定義したテキストファイルです。

製品は定義ファイルをダウンロードし、バージョン変更の必要があると判断した場合のみ、プログラムファイルのダウンロードを行います。この機能により、不必要な通信を軽減し、無線経由でダウンロードする場合のパケット料金を抑えることができます。

定義ファイルは、半角コロンで区切られたCSVフォーマットを用います。

以下のフォーマットで記載します。

＃ コメント行

「バージョン情報」，URL(「プログラムファイル」まで指定する)

例）

```
# WA1020 最新プログラムファイル
5.1.2,http://www.example.com/program/wa1020_5_1_2.bin
```

● 定義ファイルを指定しない場合

定義ファイルを指定せず、直接ダウンロードするプログラムファイルを指定することができます。プログラムファイルをURLで指定した場合は、バージョン変更の必要がなくても、毎回プログラムファイルのダウンロードを行います。

```
WA1020(config)# auto-versionup firmware url
http://www.example.com/program/wa1020_5_1_2.bin [Enter]
WA1020(config)#
```

共通設定

⑤ダウンロードスケジュールの設定

ダウンロードスケジュールの設定を行います。スケジュールは、起動時指定と日時指定（定期実行）の2パターンの設定ができます。

- 起動時指定

起動直後にプログラムファイルをダウンロードします。

起動時実施の場合、FTP/HTTPサーバへのルートが存在しない可能性があるため、リトライ回数とリトライ間隔の設定を行います。

以下の例は、リトライ回数3回、リトライ間隔5秒の設定となります。

```
WA1020(config)# auto-versionup startup-execute retry 3 interval 5 [Enter]
WA1020(config)#
```

また、装置起動時からプログラムファイルのダウンロード実施までの遅延時間を設定することで、無駄なリトライを低減できます。

以下の例は、遅延時間60秒の設定となります。（初期値：30秒）

```
WA1020(config)# auto-versionup startup-delay 60 [Enter]
WA1020(config)#
```

- 日時指定（定期実行）

起動中にプログラムファイルをダウンロードします。

以下の例は、毎月15日、00:00 にダウンロードする定期実行の設定となります。

```
WA1020(config)# auto-versionup schedule monthly 15 00:00 [Enter]
WA1020(config)#
```

メモ　正しい日時に実行するため、NTPクライアント機能を利用して時刻同期を行ってください。

⑥再起動有効設定

自動バージョンアップが行われ、バージョン変更が完了した場合に、自動的に再起動を行うように設定します。

```
WA1020(config)# auto-versionup reboot-enable [Enter]
WA1020(config)#
```

メモ　ソフトウェアバージョンが同じ場合は、再起動されません。

メモ　製品の再起動スケジュール機能が有効であった場合には、自動的に再起動されません。再起動スケジュールの設定時間に再起動されます。

メモ　再起動時にSyslogバックアップを行います。

⑦自動バージョンアップ有効化

自動バージョンアップを有効化します。

```
WA1020(config)# auto-versionup enable [Enter]
WA1020(config)#
```

⑧ブートエントリの設定

ブートエントリの設定を行います。

```
WA1020(config)# boot entry flash wa1020.bin [Enter]
WA1020(config)#
```

- ブートエントリをつかわない場合

ブートエントリを使わない場合、他のプログラムファイルを削除します。

```
WA1020(config)# erase firmware FILENAME [Enter]
WA1020(config)#
```

show storageコマンドで、他のプログラムファイルが無いことを確認します。

```
WA1020(config)# show storage [Enter]
wa1020.bin      5163676 bytes
startup.conf        512 bytes
WA1020(config)#
```

■設定手順（自動コンフィグファイル更新）

以下の手順で設定を行います。FTP使用の場合は、①～④を、HTTP使用の場合は、①’～④’を実施します。スケジュール等共通設定は、両サーバとも⑤～⑦を実施します。

なお、コマンドの詳細については、コマンドリファレンスをご参照ください。

FTPサーバの場合

① FTP/HTTPサーバの設定

② FTP/HTTPログイン情報の設定

③ FTPモードの設定

④ FTPコンフィグレーションファイルの設定

HTTPサーバの場合

①’ HTTPサーバの設定

②’ HTTPログイン情報の設定

③’ HTTP BASIC認証使用/未使用の設定

④’ HTTPコンフィグレーションファイルの設定

共通設定

⑤ ダウンロードスケジュールの設定

⑥ 再起動有効設定

⑦ 自動コンフィグファイル更新の有効化

FTPサーバの場合

①FTPサーバの設定

ダウンロード先のサーバの指定を行います。

```
WA1020(config)# auto-versionup mode ftp [Enter]
WA1020(config)#
```

FTPサーバの設定を行います。ポート番号を初期値の21から変更する場合は、サーバ名の後に設定することができます。コンフィグレーションファイル更新用のFTPサーバは1つのみ設定できます。設定変更を行った場合は上書きされます。

```
WA1020(config)# auto-versionup server ftp.example.com [Enter]
WA1020(config)#
```

②FTPログイン情報の設定

FTP/HTTPサーバのアカウントパスワードを設定します。HTTPサーバの場合は、BASIC認証のアカウントになります。例では、以下を設定しています。

アカウント：wa1020

パスワード：ftppassword

```
WA1020(config)# auto-config-update authentication username wa1020[Enter]
WA1020(config)# auto-config-update authentication password plain ftppassword
[Enter]
WA1020(config)#
```

③FTPモードの設定

FTPサーバのモード（Active/Passive）を設定します。FTPモードの初期値はpassiveです。FTPモードを変更しない場合は設定する必要はありません。

```
WA1020(config)# auto-config-update ftpmode passive [Enter]
WA1020(config)#
```

④FTPコンフィグレーションファイルの設定

コンフィグレーションファイルの設定を行います。

コンフィグレーションファイルのファイル名、およびディレクトリを設定します。

例では、以下を設定しています。

保存ディレクトリ（保存パス）：wa1020/program

コンフィグレーションファイル：wa1020_conf.txt

```
WA1020(config)# auto-config-update configfile wa1020_conf.txt[Enter]
WA1020(config)# auto-config-update configfile path wa1020/program [Enter]
WA1020(config)#
```

また、ダウンロードするコンフィグレーションファイルに、レビジョンコマンドの記載が必要です。（auto-config-update revision コマンドでレビジョン指定が必須）

HTTPサーバの場合

①’HTTPサーバの設定

ダウンロード先のサーバの指定を行います。

```
WA1020(config)# auto-versionup mode http [Enter]
WA1020(config)#
```

②' HTTPログイン情報の設定

HTTPサーバのアカウントパスワードを設定します。BASIC認証のアカウントになります。例では、以下を設定しています。

アカウント：wa1020

パスワード：ftppassword

```
WA1020(config)# auto-config-update authentication username wa1020[Enter]
WA1020(config)# auto-config-update authentication password plain ftppassword
[Enter]
WA1020(config)#
```

③' HTTP BASIC認証使用/未使用の設定

HTTPサーバの場合は、認証の使用有無を設定できます。例では、BASIC認証実施を指定します。

```
WA1020(config)# auto-versionup authentication mode basic [Enter]
WA1020(config)#
```

④' HTTPコンフィグレーションファイルの設定

コンフィグレーションファイルのURLを指定します。保存パス含めファイル名まで設定します。

例では、以下を設定しています。

URLアドレス（保存パス含） ：http://www.example.com/program/wa1020_conf.txt

コンフィグレーションファイル：wa1020_conf.txt

```
WA1020(config)# auto-config-update configfile url
http://www.example.com/program/wa1020_conf.txt [Enter]
WA1020(config)#
```

また、ダウンロードするコンフィグレーションファイルに、レビジョンコマンドの記載が必要です。（auto-config-update revision コマンドでレビジョン指定が必須）

共通設定

⑤ダウンロードスケジュールの設定

ダウンロードスケジュールの設定を行います。スケジュールは、起動時指定と日時指定（定期実行）の2パターンの設定ができます。

- 起動時指定

起動時にコンフィグレーションファイルをダウンロードします。

起動時実施の場合、FTP/HTTPサーバへのルートが存在しない可能性があるため、リトライ回数とリトライ間隔の設定を行います。

以下の例は、リトライ回数3回、リトライ間隔5秒の設定となります。

```
WA1020(config)# auto-config-update startup-execute retry 3 interval 5 [Enter]
WA1020(config)#
```

また、装置起動時からコンフィグレーションファイルのダウンロード実施までの遅延時間を設定することで、無駄なリトライを低減できます。

以下の例は、遅延時間60秒の設定となります。（初期値：30秒）

```
WA1020(config)# auto-config-update startup-delay 60 [Enter]
WA1020(config)#
```

● 日時指定（定期実行）

指定した日時にプログラムファイルをダウンロードします。

以下の例は、日時指定で「2013年9月1日 12時」 にダウンロードを実施する例です。

```
WA1020(config)# auto-config-update schedule date 2013/9/1 12:00 [Enter]
WA1020(config)#
```

メモ　正しい日時に実行するため、NTPクライアント機能を利用して時刻同期を行ってください。

⑥再起動有効設定

自動コンフィグファイル更新が行われ、スタートアップコンフィグの更新が完了した場合に、自動的に再起動を行うように設定します。

```
WA1020(config)# auto-config-update reboot-enable [Enter]
WA1020(config)#
```

メモ　製品の再起動スケジュール機能が有効であった場合には、自動的に再起動されません。再起動スケジュールの設定時間に再起動されます。

メモ　再起動時にSyslogバックアップを行います。

⑦自動コンフィグファイル更新有効化

自動コンフィグファイル更新機能を有効化します。

```
WA1020(config)# auto-config-update enable [Enter]
WA1020(config)#
```

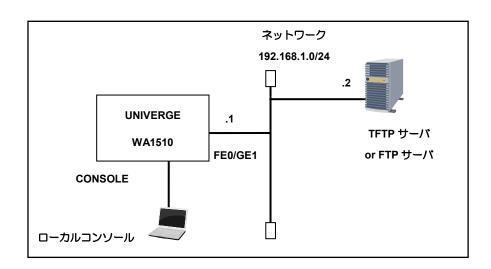
ファイル転送

本製品のTFTP／FTPクライアント機能を使用して、プログラムファイルやコンフィグレーションファイルをTFTP／FTPサーバに転送することができます。

また、USBメモリをUSBストレージとして使用し、copyコマンドでUSBメモリへ転送することができます。

以下のネットワーク構成におけるプログラムファイルのバックアップとコンフィグレーションファイルのファイル転送について説明します。

メモ　FTPクライアントはソフトウェアバージョン 2.2から対応しています。

メモ　USBストレージ機能は、ソフトウェアバージョン 5.1から対応しています。

以下では代表例としてWA1510の場合の手順を説明します。

■プログラムファイルのバックアップ

①バックアップするプログラムファイルの確認

show storage コマンドを使用してバックアップを行うプログラムファイルのファイル名を確認します。

```
WA1500# show storage [Enter]
wa1500_5_1_0.bin     4936400 bytes
wa1500_5_0_4.bin     4753140 bytes
startup.conf        896 bytes

total 132775936 bytes, avail 118038208 bytes
WA1500#
```

②バックアップするプログラムファイルを TFTP サーバ／FTP サーバへファイル転送

tftp put / ftp putコマンドを使用して、指定したプログラムファイルをTFTPサーバもしくはFTPサーバにアップロードします。アップロード中は、「#」にて進行状況を確認することができます。

● TFTPサーバへのアップロード

以下の例では、バージョンが 5.0.4 のプログラムファイルを転送しています。

```
WA1500# tftp put wa1500_5_0_4.bin 192.168.1.2:wa1500_5_0_4.bin [Enter]
connect  to192.168.1.2 ...
###########################################################################
###########################################################################
###########################################################################
###########################################################################
###########################################################################
###########################################################################
###########################################################################
###########################################################################
###########################################################################
###########################################################################
###########################################################################
###########################################################################
###########################################################################
###############
WA1500#
```

● FTPサーバへのアップロード

以下の例では、ユーザ名をwa1020、パスワードをftppasswordのアカウントでバージョンが 5.1.2 のプログラムファイルを転送しています。

```
WA1500# ftp put wa1500_5_1_0.bin 192.168.1.2:wa1500_5_1_2.bin wa1020
ftppassword [Enter]
connect to 192.168.1.2 ...###############################################
WA1500#
```

メモ　転送後は、tftp/ftpサーバにて、ファイル名とファイルサイズを確認し、プログラムファイルが正常にアップロードできたことを確認します。

②'バックアップするプログラムファイルを USB ストレージへファイル転送

copyコマンドを使用して、指定したプログラムファイルをUSBストレージにアップロードします。

● USBストレージへのアップロード

以下の例では、出荷時登録のプログラムファイルを転送しています。

```
WA1500# copy wa1500.bin usb-storage wa1500.bin [Enter]
Copy to wa1500.bin
WA1500#
```

メモ　プログラムファイルの転送先USBストレージでのファイル名を省略すると、同じファイル名でアップロードします。ファイル名が存在する場合は、上書きの確認を行います。

メモ　転送後は、show usb-storageコマンドで、ファイル名とファイルサイズを確認し、プログラムファイルが正常にアップロードできたことを確認します。

```
WA1500# show usb-storage [Enter]
  2014/03/07 06:43:10 wa1500.bin                        4861036 bytes

total 491648 Kbytes, avail 486896 Kbytes
WA1500#
```

■USB ストレージからプログラムファイルのバックアップ

USBストレージへバックアップしたプログラムファイルをさらにTFTP/FTPサーバへ転送することができます。

①バックアップする USB ストレージ上のプログラムファイルの確認

show usb-storage コマンドを使用してバックアップを行うプログラムファイルのファイル名を確認します。

```
WA1500# show usb-storage
  2014/03/07 05:43:10 wa1500.bin                        4861036 bytes

total 491648 Kbytes, avail 486896 Kbytes
WA1500#
```

②バックアップするプログラムファイルを TFTP サーバ／FTP サーバへファイル転送

tftp put / ftp putコマンドを使用して、指定したプログラムファイルをTFTPサーバもしくはFTPサーバにアップロードします。アップロード中は、「#」にて進行状況を確認することができます。

- TFTPサーバへのアップロード

以下の例では、出荷登録のプログラムファイルを転送しています。

```
WA1500# tftp put usb-storage wa1500.bin 192.168.1.2:wa1500.bin [Enter]
connect to 192.168.1.2 ...################################################
#########################################################################
#########################################################################
#########################################################################
#########################################################################
#########################################################################
#########################################################################
#########################################################################
#########################################################################
#########################################################################
#########################################################################
#########################################################################
#########################################################################
#########################
WA1500#
```

● FTPサーバへのアップロード

以下の例では、ユーザ名をwa1020、パスワードをftppasswordのアカウントで出荷登録のプログラムファイルを転送しています。

```
WA1500# ftp put usb-storage wa1500.bin 192.168.1.2:wa1500.bin wa1020
ftppassword [Enter]
connect to 192.168.1.2 ...################################################
WA1500#
```

メモ　転送後は、tftp/ftpサーバにて、ファイル名とファイルサイズを確認し、プログラムファイルが正常にアップロードできたことを確認します。

■コンフィグレーションファイルのファイル転送

コンフィグレーションファイルを TFTP サーバ／FTP サーバへファイル転送

tftp put / tfp putコマンドを使用して、現在のコンフィグレーションファイルをTFTPサーバもしくはFTPサーバにアップロードすることで、コンフィグレーションファイルのバックアップを行えます。

- TFTPサーバへのアップロード

```
WA1500# tftp put startup-config 192.168.1.2:startup.conf
connect to 192.168.1.2 ...
WA1500# 
```

- FTPサーバへのアップロード

```
WA1500# ftp put startup-config 192.168.1.2:startup.conf wa1020 ftppassword
connect to 192.168.1.2 ...
WA1500# 
```

TFTP サーバ／FTP サーバからコンフィグレーションファイルを取得

tftp get / ftp getコマンドを使用して、TFTPサーバもしくはFTPサーバからコンフィグレーションファイルをダウンロードすることで、スタートアップコンフィグの書き換えが可能です。

- TFTPサーバからのダウンロード

```
WA1500# tftp get 192.168.1.2:startup.conf startup-config
connect to 192.168.1.2 ...
Update startup-config file ...
WA1500# 
```

- FTPサーバからのダウンロード

```
WA1500# ftp get 192.168.1.2:startup.conf startup-config wa1020 ftppassword
connect to 192.168.1.2 ...
Update startup-config file ...
WA1500# 
```

コンフィグレーションファイルを USB ストレージへファイル転送

copyコマンドを使用して、現在のコンフィグレーションファイルをUSBストレージにアップロードすることで、コンフィグレーションファイルのバックアップを行えます。

- USBストレージへのアップロード

```
WA1500# copy startup-config usb-storage startup.conf [Enter]
Save to startup.conf
WA1500# 
```

USB ストレージからコンフィグレーションファイルを取得

copyコマンドを使用して、USBストレージからコンフィグレーションファイルをダウンロードすることで、スタートアップコンフィグの書き換えが可能です。

● USBストレージからのダウンロード

```
WA1500# copy usb-storage startup-config startup.conf startup.conf [Enter]
Copy to startup.conf
WA1500#
```

USB ストレージのコンフィグレーションファイルを TFTP サーバ／FTP サーバへファイル転送

tftp put / ftp putコマンドを使用して、USBストレージ上のコンフィグレーションファイルをTFTPサーバもしくはFTPサーバにアップロードすることで、コンフィグレーションファイルのバックアップを行えます。

また、syslogのバックアップファイル、テクニカルサポート情報(show technical-support)ファイルも転送が可能です。

● TFTPサーバへのアップロード

```
WA1500# tftp put usb-storage startup.cnf 192.168.1.2:startup.cnf [Enter]
connect to 192.168.1.2 ...
WA1500#
```

● FTPサーバへのアップロード

```
WA1500# ftp put usb-storage startup.cnf 192.168.1.2:startup.cnf wa1020
ftppassword [Enter]
connect to 192.168.1.2 ...#
WA1500#
```

TFTP サーバ／FTP サーバから USB ストレージへコンフィグレーションファイルを取得

tftp get / ftp getコマンドを使用して、TFTPサーバもしくはFTPサーバからコンフィグレーションファイルをUSBストレージへダウンロードすることで、直接コンフィグレーションファイルを書き換えないローカルでの保存ができます。

● TFTPサーバからのダウンロード

```
WA1500# tftp get usb-storage 192.168.1.2:startup-conf.txt startup.conf
[Enter]
connect to 192.168.1.2 ...
WA1500#
```

● FTPサーバからのダウンロード

```
WA1500# ftp get usb-storage 192.168.1.2:startup-conf.txt startup.conf wa1020
ftppassword [Enter]
connect to 192.168.1.2 ...#
WA1500#
```

注意　本製品のスタートアップコンフィグを書き換える場合、コンフィグレーションファイル名には、アスキー文字を使用してください。

メモ　show startup-config または show running-config コマンドを使用して設定内容をコンソール画面上に表示し、このログを保存しておくことでテキストファイルによる管理も可能です。
このテキストファイルから必要な設定をカット＆ペーストすることで本製品の設定を行うことが可能です。

装置内情報の確認

WA1510、WA1511にて、以下の情報が追加になります。

- ブートソフトウェアバージョン
- 内蔵モジュールの型名表示
- 装置起動時の自己診断テスト結果表示
- 装置内の温度表示

■ブートソフトウェアバージョンと内蔵モジュールの表示

WA1510、WA1511では、ブートソフトウェアのバージョン、内蔵モジュールの有無と型番をshow versionコマンドにて確認することができます。

WA1510の画面例を以下に示します。

```
WA1500# show version [Enter]
Copyright (c) NEC Platforms, Ltd. 2013 All rights reserved.
Copyright (c) 1996-2004
   The NetBSD Foundation, Inc.  All rights reserved.
Copyright (c) 1982, 1986, 1989, 1991, 1993
   The Regents of the University of California.  All rights reserved.
Bootstrap Software       : version 1.0.1
Operating System Software : version 5.0.0
Compiled:  Fri Dec 20 14:06:48 JST 2013

Serial Number: 13*******

Embedded Module: none
uptime is 0 days 0 hours 0 minutes 19 secs.
memory size is 134217728 [byte]
WA1500#
```

①ブートソフトウェアバージョンの表示

②内蔵モジュールない場合

WA1511の画面例を以下に示します。

```
WA1500# show version [Enter]
Copyright (c) NEC Platforms, Ltd. 2013 All rights reserved.
Copyright (c) 1996-2004
   The NetBSD Foundation, Inc.  All rights reserved.
Copyright (c) 1982, 1986, 1989, 1991, 1993
   The Regents of the University of California.  All rights reserved.
Bootstrap Software       : version 1.0.1
Operating System Software : version 5.0.0
Compiled:  Fri Dec 20 14:06:48 JST 2013

Serial Number: 13*******

Embedded Module: HM-M100
uptime is 0 days 0 hours 0 minutes 19 secs.
memory size is 134217728 [byte]
WA1500#
```

③内蔵モジュール型番表示

メモ　他の装置の場合は、コンソール接続して装置を起動または、再起動することで、コンソールにブートソフトウェアのバージョンが表示されます。

■装置起動時の自己診断テスト結果表示

WA1510、WA1511では、装置起動時に動作する自己診断の結果をshow diagnosticsコマンドにて確認することができます。
今までは、コンソールを接続後、起動または再起動することで確認していた内容を起動後に確認できます。

WA1511の画面例を以下に示します。

```
WA1500# show diagnostics [Enter]
Power On Self Test(POST) information
  RTC  TEST   : OK
  WAN  TEST   : OK
  LAN  TEST   : OK
  USB  TEST   : OK
  TEMP TEST   : OK
  SEC  TEST   : OK
  MODEL check : OK

Memory information
  total size : 256MB

Flash information
  total 132775936 bytes, avail 123278528 bytes

Embedded module information
  HM-M100
WA1500#
```

自己診断の結果で”NG”表記箇所がある場合は、ハードウェアの問題が考えられます。
販売元にご連絡ください。

■装置内の温度表示

WA1510、WA1511では、装置内の温度表示をshow environmentコマンドにて確認することができます。

show environmentコマンドの画面例を以下に示します。

```
WA1500# show environment [Enter]
System hardware information:

  Internal temperature measured at 49.21C
  Status is normal
WA1500#
```

historyオプションにて、電源起動時からコマンド入力時点までの間の最高温度と最低温度を表示することができます。

オプション指定での画面例を以下に示します。

```
WA1500# show environment history [Enter]
System hardware information:

  Internal temperature measured at 49.28C
  Status is normal

  maximum 49.28C 2014/01/19 06:00:41
  minimum 49.21C 2014/01/19 06:00:36
WA1500#
```

メモ　装置内温度は、プライベートMIBでも取得可能です。

表示温度値が異常値(Status is abnormal)の場合は、設置環境の温度が保証範囲外、または装置の通気口が塞がれているなどの可能性がありますので、装置周辺の空間確保や、装置周囲の温度を下げるなどの対策を行ってください。

メモ　温度異常を検出した場合に、syslog表示させる場合は、本章の”イベント情報収集の設定”をご確認ください。

SNMPによる管理

本製品は、ネットワーク管理プロトコルとして SNMP（Simple Network Management Protocol）を使用可能ですので、SNMP マネージャにて本製品の MIB 情報の取得が可能です。また、重要なイベントが発生した際に､トラップ情報を SNMP マネージャに送信することでイベント情報を管理者に通知可能です。
取得可能な MIB 情報は、標準 MIB に加えデータ通信端末の状態を SNMP マネージャで取得できるプライベート MIB をサポートしています。

注意　SNMP マネージャから本製品の設定変更を行うことはできません。

注意　プライベート MIB は、ソフトウェアバージョン 4.0 以降で使用できます。

コミュニティ名

SNMPによるネットワーク管理にはコミュニティ名が必要となります。コミュニティ名は、SNMPマネージャから本製品へのアクセスが行われる際に確認されます。コミュニティ名はSNMPマネージャの設定にあわせて設定を行います。

トラップ情報

本製品では、SNMPマネージャに送信するトラップ情報の種別を設定可能です。
本製品がサポートするトラップ情報については､コマンドリファレンスをご参照ください。
また、複数のSNMPマネージャへのトラップ情報の送信が可能です。

プライベート MIB 情報

データ通信端末の状態を取得できるプライベートMIBは、show mobile status と show wimax status で取得できる情報及びWA1510、WA1511については、加えて show environment の装置内部温度表示で取得できる情報と同じ情報です。

取得できる情報の内容

show mobile statusコマンドで表示される情報は以下のような内容です。

機種、FWバージョン、製造番号、電話番号、USB通信モード、PIN認証実行状態、PIN認証結果、アンテナレベル、アンテナ圏内圏外情報、サービス情報、リカバリ実施数、データ通信端末制御情報、リカバリ有効無効状態、USB0状態（WAシリーズ共通）、USB1状態（WA2020とWA2021）、module0状態（WA1511）、回線交換時の発呼制限情報など

show wimax statusコマンドで表示される情報は以下のような内容です。

機種、FWバージョン、端末のMACアドレス、電波レベル、WiMAX回線接続状態、リカバリ有効無効状態

SNMPマネージャに WA-SMI.mib.txt を適用することで､プライベートMIBを取得できます。
WA-SMI.mib.txtの詳細は、販売元にお問い合わせください。

■設定手順

設定は以下の手順で行います。

なお、SNMP関連コマンドの詳細は、コマンドリファレンスをご参照ください。

① コミュニティ名の設定

② トラップ送信先の設定

③ 送信トラップ種別の設定

④ SNMPエージェントの起動

⑤ 動作確認

以下では代表例としてWA1020の場合の手順を説明します。

①コミュニティ名の設定

コミュニティ名とアクセスタイプを設定します。

アクセスタイプの設定は、read-only（MIB読み出し）のみ指定可能です。

以下の例では、コミュニティ名に「public」を設定しています。

```
WA1020(config)# snmp community public read-only [Enter]
WA1020(config)#
```

注意　セキュリティを高めるために、単純なコミュニティ名の使用を避けてください。

②トラップ送信先の設定

トラップ情報を送信するSNMPマネージャのIPアドレスを設定します。

設定能な送信先IPアドレスは最大8件です。

以下の例では、SNMPマネージャのアドレスを192.168.1.100としています。

```
WA1020(config)# snmp trap destination 192.168.1.100 public [Enter]
WA1020(config)#
```

③送信トラップ種別の設定

送信するトラップ情報の種別を設定します。

以下の例は、「link-up」トラップの送信を行う場合です。

```
WA1020(config)# snmp trap public generic-trap link-up [Enter]
WA1020(config)#
```

④SNMP エージェントの起動

SNMPエージェントを起動することで、SNMPマネージャによる本製品のMIB情報取得や、本製品からのトラップ送信が可能となります。SNMPマネージャに WA-SMI.mib.txt を適用することで、プライベートMIBを取得できます。

```
WA1020(config)# snmp enable [Enter]
WA1020(config)#
```

⑤動作確認

SNMPマネージャから本製品のMIB情報が取得可能なこと、あるいはイベント発生時にトラップが正常に送信されるかを確認します。

イベント情報収集の設定

製品稼働中に発生するイベント情報や障害解析に必要な情報を収集します。
イベント情報種別、イベント情報レベル、イベント情報の出力先が設定可能です。

イベント情報種別は、以下となります。

all	：全機能
aaa	：ログイン認証、権限遷移など
acl	：アクセスリスト
arp	：ARP
bridge	：Bridge
chat	：CHAT
cnmgr	：WiMAX接続制御
config	：コンフィグ設定
ddns	：DDNSクライアント
dhcp4c	：DHCPv4クライアント
dhcp4r	：DHCPv4リレー
dhcp4s	：DHCPv4サーバ
env	：温度表示(WA1510とWA1511)
etherip	：EtherIP
ftp	：FTPクライアント
http	：Web-GUI
if	：インタフェース
ike	：IKE
ip	：経路制御
ipsec	：IPsec
l2tp	：L2TPv3
mail	：Mail
mobeth	：モバイルイーサー
mobethb	：モバイルイーサーブリッジ（WA1020のみ）
mobile	：モバイルモデム
nat	：NAT
netmon	：ネットワークモニタ
ntp	：NTP
pdns	：プロキシDNS

ppp	：PPP
pppb	：PPP Bridge（WA1020のみ）
pppoe	：PPP over Ethernet（WA1510、WA1511、WA2020、WA2021）
snmp	：SNMP
sshsv	：SSHサーバ
storage	：ストレージ
telsv	：Telnetサーバ
tftp	：TFTPクライアント
verup	：FTP自動バージョンアップ
vlan	：VLAN
vrrp	：VRRP
wimax	：WiMAX
wimaxb	：WiMAXブリッジ（WA1020のみ）
wlan	：無線LAN（WA2021のみ）

イベント情報のレベル（プライオリティ）は、以下となります。

emergency	：システムダウンなどの非常事態
alert	：緊急に対処すべきエラー
critical	：致命的なエラー
error	：一般的なエラー
warning	：注意喚起すべき情報
notice	：一般的な情報
information	：参考となる付加的な情報
debug	：デバッグ情報

イベント情報の出力先は、以下に対応しています。

- ローカルコンソール／リモートコンソール（Telnet）
- DRAM（フラッシュメモリ/USBストレージへのバックアップが可能）
- Syslogサーバ
- メール送信

注意　イベント情報を収集する場合は、必要とする情報種別とレベルのみ設定を行ってください。不要なイベント情報の収集は、本製品の負荷を上げることになります。
特にデバッグレベルで多くのイベント情報種別を収集する場合は、多量のイベント

情報を収集することになるため、本製品が過負荷状態になりますのでご注意ください。

注意 IPsecやEtherIPなどの機能を用いてイベント情報を送信する場合、Syslogサーバへ送信するパケットについてもロギングが行われます。パケット自体がロギングされるイベント情報を指定しないでください。

以下では代表例としてWA1020の場合の手順を説明します。

■収集するイベント情報の設定

以下の例では、イベント情報種別に「mobile」、イベント情報レベルに「デバッグ」レベルを指定しています。

また、イベント情報のタイムスタンプは、「datetime」（イベント情報の発生年月日と時刻）を指定しています。

```
WA1020(config)# syslog function mobile debug [Enter]
WA1020(config)# syslog time-stamp datetime [Enter]
WA1020(config)#
```

メモ イベント情報に時刻を記録する場合は、時刻情報の手動設定あるいはNTPによる時刻同期設定を行ってください。

メモ 本製品のACアダプタの電源プラグをACコンセントから抜くと、WA1020では時刻設定は次回の電源投入時に初期化されますが、WA1510、WA1511では約5日間保持、WA2020、WA2021では約10日間保持されます。
WA1020/WA1510/WA1511/WA2020/WA2021のいずれも時刻が初期化された場合は再度設定を行ってください。

■イベント情報の収集開始

イベント情報を収集するためにSyslog機能を有効にします。

```
WA1020(config)# syslog enable [Enter]
WA1020(config)#
```

■イベント情報の出力

イベント情報の出力先は、ローカルコンソール／リモートコンソール（Telnet）、

フラッシュメモリ、Syslogサーバを設定可能です。

<u>過去のイベント情報をコンソール画面に表示する</u>

過去に発生したイベント情報はDRAMに保存され、show syslogコマンドで表示することができます。

```
WA1020(config)# show syslog [Enter]
2009-06-30 07:46:40 MOBILE.INFO Modem attached on USB port
2009-06-30 07:46:40 MOBILE.INFO modem DCD change -> ON
2009-06-30 07:46:40 MOBILE.INFO name: xxxxx
2009-06-30 07:46:40 MOBILE.INFO version: x.x.x.x.x
2009-06-30 07:46:40 MOBILE.INFO serialnumber: xxxxxxxxxxxxxxx
2009-06-30 07:46:40 MOBILE.INFO pin: +CPIN: READY
2009-06-30 07:46:47 MOBILE.INFO mynumber: +CNUM: "","xxxxxxxxxxx",129
2009-06-30 07:46:48 MOBILE.INFO antenna status change 0 -> 4
WA1020(config)#
```

イベント情報をコンソール画面にリアルタイム表示する（デバッグ機能）

イベント情報のリアルタイム表示開始と停止は特権モードで行います。

syslog functionコマンドで設定されているイベントが発生するとコンソール画面に表示されます。

イベント情報のリアルタイム表示を停止するときは、debug stopコマンドで行います。

```
WA1020# debug start [Enter]
WA1020#
WA1020#
2009-06-30 07:46:40 MOBILE.INFO Modem attached on USB port
2009-06-30 07:46:40 MOBILE.INFO modem DCD change -> ON
2009-06-30 07:46:40 MOBILE.INFO name: xxxxx
2009-06-30 07:46:40 MOBILE.INFO version: x.x.x.x.x
2009-06-30 07:46:40 MOBILE.INFO serialnumber: xxxxxxxxxxxxxxx
2009-06-30 07:46:40 MOBILE.INFO pin: +CPIN: READY
2009-06-30 07:46:47 MOBILE.INFO mynumber: +CNUM: "","xxxxxxxxxxx",129
2009-06-30 07:46:48 MOBILE.INFO antenna status change 0 -> 4
```

メモ　コマンド入力中に本製品がイベントを検出した場合、イベントメッセージがコマンドに続けて表示され、途中まで入力したコマンドが画面から消えることがありますが、本製品は途中まで入力したコマンドを記憶していますので、最初から入力し直す必要はありません。そのまま続けて入力可能です。

イベント情報をバックアップする（Syslog バックアップ機能）

イベント情報をバックアップする為に、以下の二つの機能が用意されています。運用目的に応じて選択が可能です。

- 1日1回、DRAMに保存している最新のイベント情報から128Kbyte分をフラッシュメモリに格納します。一時的なバックアップに適しています。
- DRAMに保存しているイベント情報が規定値を越えたとき、USBストレージに格納します。出力したイベント情報を漏れなくバックアップ出来ます。
  オプションのUSBメモリが必要です。

以下に設定と動作について説明します。

● イベント情報を1日１回フラッシュメモリに保存する機能

DRAMに保存されているイベント情報を１日１回指定した時刻にフラッシュメモリに保存します。フラッシュメモリに保存できるサイズは128Kbyteとなっており、DRAM上で保存されているイベント情報の最新のイベントから128Kbyte分までが格納されます。

なお、DRAM上で保存できるサイズは、512Kbyteとなっています。容量が超過すると古いイベント情報から順に削除されます。

以下の例では、保存時刻を 「23:00」 に指定しています。

```
WA1020(config)# syslog backup time 23:00 [Enter]
WA1020(config)# syslog backup enable [Enter]
WA1020(config)#
```

メモ　保存されたイベント情報は製品起動時にDRAMへ読み込みを行い、show syslog コマンドにて確認できます。

メモ　バックアップ実施時点から次のバックアップが実施されるまでの間に、本製品の電源OFFや再起動が行われると、その期間におけるイベント情報は失われます。

● イベント情報をUSBストレージに保存する機能

DRAMに保存されているイベント情報をUSBストレージに保存します。DRAM保存量が規定の容量を超えるとUSBストレージに保存します。USBストレージの空き容量が書き込み可能容量(残30Mbyte)以下になるとバックアップを停止します。

本機能は、ソフトウェアバージョン5.1以降で使用できます。

バックアップ時のファイル名は、以下となります。

バックアップファイル名：syslog_DATE_time.txt(syslog_YYYYMMDD_HHMMSS.txt)

以下の設定で、syslogをUSBストレージにバックアップを開始します。

```
WA1020(config)# syslog backup usb-storage enable [Enter]
WA1020(config)#
```

注意　バックアップ実施時点から次のバックアップが実施されるまでの間に、本製品の電源OFFや再起動が行われると、その期間におけるイベント情報は失われます。

イベント情報を Syslog サーバに送信する（Syslog クライアント機能）

syslog functionコマンドで設定されているイベント情報を、Syslogサーバへ送信します。Syslogサーバへの送信設定は、グローバルコンフィグモードにおいてSyslogコマンドで行います。例では、Syslogサーバのアドレスに「192.168.1.1」を設定しています。

```
WA1020(config)# syslog destination 192.168.1.1 [Enter]
WA1020(config)#
```

イベント情報をメール送信する

DRAMに保存されているイベント情報をメールの本文として引用し、特定のホストに送信できます。最新のイベントから指定された容量分までのイベントをメールに引用できます。

```
WA1020(config)#
WA1020(config)# syslog enable  [Enter]
WA1020(config)# syslog mail time 19:00  [Enter]
WA1020(config)# syslog mail size 5000  [Enter]
WA1020(config)# syslog mail enable [Enter]
WA1020(config)# syslog function all debug [Enter]
WA1020(config)#
WA1020(config)# smtp profile test [Enter]
WA1020(config)# mail address to admin@example.jp from user@example.jp [Enter]
WA1020(config)# mail authentication method smtp-auth [Enter]
WA1020(config)# mail authentication id user@example.jp [Enter]
WA1020(config)# mail authentication password encrypted
0x2757262c2b4642273f4c434e4026 [Enter]
WA1020(config)# smtp-server smtp.example.jp 587 mode smtp-over-tls [Enter]
WA1020(config)#
WA1020(config)#
```

再起動

本製品を再起動する場合、以下の２つの方法があります。

■AC アダプタの抜き差しによる再起動

STATランプが赤点滅していないことを確認し、ACアダプタの電源プラグをコンセントから外して電源をOFFにします。その後数秒間待ってから、電源プラグをコンセントに差し込んでください。

注意　現在動作中のランニングコンフィグは消去されますので、必要に応じて再起動前に設定保存を行ってください。

注意　製品本体とACアダプタ間のDCジャックの挿抜による電源の切断は行わないでください。

■reboot コマンドによる再起動

ローカルコンソール／リモートコンソールから、特権モードにて rebootコマンドにより行います。

```
WA1020# reboot [Enter]
Are you sure you want to reboot the router? (Yes or [No]): y [Enter]
# reboot....

IPL: SOFT-RESET
IPL: MEMORY OK

Boot: Version 1.0.0
POST:
DRAM Test ..... PASS
TClock Test ... PASS
FLASH CHKSUM .. PASS
LAN Test ..... PASS
PCI Test ..... PASS
3DES->HMAC-SHA1 TEST ... PASS
AES256->HMAC-SHA1 TEST ... PASS
DES->HMAC-MD5 TEST ... PASS
3DES->HMAC-MD5 TEST ... PASS
AES128->HMAC-MD5 TEST ... PASS
AES192->HMAC-MD5 TEST ... PASS
AES256->HMAC-MD5 TEST ... PASS
NULL->HMAC-MD5 TEST ... PASS
post success
LM: loading "wa1020_1_0_0.bin"
............................................................
Tue Jun 30 13:58:35 JST 2009

WA1020 console

login:
```

初期化

アドミニストレータ権限ユーザのパスワードを忘れてしまった場合など、すべての設定データを工場出荷時の設定に戻したいときに初期化を行います。

注意　初期化を行うと、ランニングコンフィグ、スタートアップコンフィグの設定情報もすべて消去されます。

■初期化スイッチを使用する方法

本製品の初期化スイッチを押下しながら AC アダプタの電源プラグをコンセントに接続してください。

そのまま初期化スイッチを押下し続けると、WA1020、WA1510、WA1511の場合はPWR、STAT、PPP、MODEの4つのLEDが同時に3回点滅して、初期化開始をお知らせします。WA2020、WA2021の場合はPWR、STAT、PPPの3つのLEDが同時に3回点滅し、初期化開始をお知らせします。いずれの装置の場合も、LEDが3回点滅した後に初期化スイッチを放してください。

初期化が完了すると、本製品は自動的に再起動を行い、工場出荷時の設定で起動します。

■ブートモニタを使用する方法

次項目「ブートモニタ」をご参照ください。

ブートモニタ

コンフィグレーション設定を初期化したい場合や、起動時に読み込むプログラムファイルを指定して本製品の起動を行う場合などで使用します。
以下では代表例としてWA1020の場合の手順を説明します。

■ブートモニタでの初期化手順

本製品の起動直後に**[Ctrl]+c**を押下することでブートモニタに移行します。
ブートモニタのコマンドプロンプト「(boot)>」が表示されるまで**[Ctrl]+c**を押下します。

```
IPL: HARD-RESET
IPL: MEMORY OK

Boot: Version 1.0.0
POST:
DRAM Test ..... PASS
TClock Test ... PASS
FLASH CHKSUM .. PASS
LAN Test ..... PASS
PCI Test ..... PASS
3DES->HMAC-SHA1 TEST ... PASS
AES256->HMAC-SHA1 TEST ... PASS
DES->HMAC-MD5 TEST ... PASS
3DES->HMAC-MD5 TEST ... PASS
AES128->HMAC-MD5 TEST ... PASS
AES192->HMAC-MD5 TEST ... PASS
AES256->HMAC-MD5 TEST ... PASS
NULL->HMAC-MD5 TEST ... PASS
post success
LM: loading "wa1020_1_0_0.bin"
LM: key abort
Bootmonitor Mode
(boot)>
```

ccコマンドを実行し、スタートアップコンフィグを削除します。

```
boot> cc [Enter]
Are you sure you want to delete config? (Yes or [No]) : yes [Enter]
boot>
```

bコマンドを実行し、プログラムファイルのロードを開始します。

```
(boot)> b [Enter]

LM: loading "wa1020_1_0_0.bin"
............................................................
Tue Jun  30 00:00:04 JST 2009

WA1020 console

login:
```

■起動時に読み込むプログラムファイルを指定して起動

本製品の起動直後に**[Ctrl]+c**を押下することでブートモニタに移行します。

ブートモニタのコマンドプロンプト 「(boot)>」が表示されるまで**[Ctrl]+c**を押下します。

```
IPL: HARD-RESET
IPL: MEMORY OK

Boot: Version 1.0.0
POST:
DRAM Test ..... PASS
TClock Test ... PASS
FLASH CHKSUM .. PASS
LAN Test ..... PASS
PCI Test ..... PASS
3DES->HMAC-SHA1 TEST ... PASS
AES256->HMAC-SHA1 TEST ... PASS
DES->HMAC-MD5 TEST ... PASS
3DES->HMAC-MD5 TEST ... PASS
AES128->HMAC-MD5 TEST ... PASS
AES192->HMAC-MD5 TEST ... PASS
AES256->HMAC-MD5 TEST ... PASS
NULL->HMAC-MD5 TEST ... PASS
post success
LM: loading "wa1020_1_0_0.bin"
LM: key abort
Bootmonitor Mode
(boot)>
```

mbコマンドを実行し、プログラムファイルのロードを開始します。

以下の例では、TFTPサーバ（192.168.1.2）上のプログラムファイル（wa1020_1_0_0.bin）を指定して起動しています。

```
(boot)> mb net 192.168.1.2 wa1020_1_0_0.bin 192.168.1.1/24 [Enter]
connect to 192.168.3.5 ......############################################
########################################################################
################################################## 2750048 bytes Received.

module load complete
.................................................................
Tue Jun 30 18:40:25 JST 2009

WA1020 console

login:
```

7

困ったときには

起動しないときは

本製品が起動しないときには、以下の項目を確認し、対処してください。

■製品前面の STAT ランプが赤点灯/消灯を繰り返す場合

電源投入時の自己診断でSTATランプが赤点灯し、5秒程度で消灯し、再度点灯をくり返す場合、ハードウェアの問題が考えられます。ローカルコンソールを接続して問題の箇所を確認し、販売元にご連絡ください。

■製品前面のランプが 1 つも点灯していない場合

DCジャックが正しくつながっているか、ACアダプタの電源プラグがACコンセントに接続されているか確認してください。ACタップに接続されている場合はタップが接続されているか確認してください。接続が正しいのにランプが1つも点灯しないときは、販売元にご連絡ください。

■ブートモニタ画面になっている場合

ファイルシステム内のすべてのプログラムファイルを誤って削除、もしくは破壊された場合、本製品は起動できなくなり、以下のようなブートモニタの画面になります。

```
Bootmonitor Mode
(boot)>


(boot)>
```

このような場合は、ネットワークブート機能により、TFTPサーバからプログラムファイルを転送し起動することができます。

詳細は、前章の「ブートモニタ」項目をご参照ください。

ローカルコンソールが使用できないときは

以下の点を確認してください。

1） コンソールケーブルは添付の専用コンソールケーブルを使用していますか？

2） ローカルコンソールの通信設定は正しいですか?
（「2章 各部の名称とはたらき」をご参照ください。）

3） 本製品の電源はONになっていますか?

Web-GUIが使用できないときは

以下の点を確認してください。

1） PCと本装置が正しく接続されていますか？
PCと本装置の接続を確認してください。

2） 端末からpingを実施して装置からの応答がありますか？

3） InternetExploler以外のWWWブラウザを使用していませんか？
InternetExploler以外のブラウザは動作の確認をしていません。InternetExplolerをご利用ください。

4） WWWブラウザでのURL指定は、正しいでしょうか？
httpsと指定しているか、ポート番号が正しい値かを確認してください。

5） WWWブラウザの設定で、Javaアプレット、アクティブスクリプトが使用できるように設定されていますか？
Web-GUIマニュアルを確認して、端末の設定を確認してください。

6） WAN側からの接続の際、NAPTを使用している場合はWeb-GUIを使用するように設定していますか？
また、アクセスリストで許可されたIPアドレスまたはポートからの接続かどうかをご確認ください。

7） httpサーバを停止していませんか？
コンソールから、http有効化のコマンドが設定されているかご確認ください。

8） 工場出荷状態からの接続の場合、WA1020は端末を接続してもIPアドレスを自動取得できる様に設定していません。Web-GUIマニュアルを確認して、端末にIPアドレスを設定してください。

データ通信端末でWANに接続できないときは

ローカルコンソールから、設定の確認、WANの状態を確認します。Mobileランプ(PCランプ、USBランプ)、PPPランプでも状況確認できます。

1） 使用されているデータ通信端末が本製品にてサポートしている機種かご確認ください。サポートしている機種の場合、プログラムファイルのバージョンを確認いただき、当該データ通信端末をサポートしているバージョンかどうかご確認ください。

2） PPP接続の場合は、show pppで接続エラーや認証のエラー等がないか確認をしてください。エラーがある場合は、PPP関連の設定を確認してください。アダプタモードの場合は、配下のルータの設定が間違っていないかも確認してください。

3） show mobile status, show mobile statisticsでアンテナ状態、エラーの有無、データ通信端末を認識しているか等の状態を確認してください。

メモ　エラー表示は、データ通信端末に異常状態が発生した場合のみ表示されます。エラー表示を確認し、対処をお願いします。

エラー表示	対処方法
USB OVER CURRENT	USBに過電流が発生したためUSBポートが利用できません。USB機器を外して、装置の再起動を実施してください。
MODEM NOT READY	データ通信カードが利用できない状態です。データ通信カードが正しく接続されているか確認して、装置を再起動してください。
MODEM ERROR	データ通信端末からの応答がありません。dead_countがカウントアップを続ける場合は、給電OFF/ONコマンドもしくは、装置の再起動を実施してください。
SIM ERROR	SIMカードが正しく認識されないか異常な状態です。 正しいSIMカードが挿入されているか確認してください。
SIM PIN WAIT	PIN認証が有効の状態でPINコード入力待ち状態です。 正しいPINコードの登録を行い装置の再起動をしてください。
SIM LOCKED	PIN認証が3回失敗し、データ通信端末が「PINロック状態」です。 本装置では「PINロック状態」の解除は出来ません。データ通信端末の付属ツールを使用するか、事業者にご確認ねがいます。
ANTENNA LEVEL INVALID	アンテナレベルが正常に取得できない状態です。この状態が継続する場合は、装置を再起動してください。
ANTENNA LEVEL ZERO	アンテナレベルが0またはサービスエリア圏外のため通信ができない状態です。サービスエリア内で電波が届いていることを確認してください。

	サービスエリア内にもかかわらずこの状態が継続する場合は、モバイル通信網の工事などによる影響が考えられますので、モバイル通信事業者にお問い合わせください。

4） show interfacesを確認して、IPアドレスの取得とデータのやり取りを開始しているか確認してください。PPP接続の場合、Serial0を確認してください。NDIS接続の場合、MobileEthernet0.0を確認してください。

5） NDIS接続の場合、show ip dhcp-clientでdhcpサーバから取得した情報を確認してください。

6） WiMAX接続の場合は、show wimax statusでアンテナ状態、運用ステータス、データ通信端末を認識しているか等の状態を確認してください。

```
WA1020(config)# sh wimax status
 card name    : NEC AccessTechnica,Ltd. AtermWM3200U, rev 2.00/0.01, addr 2
 version      : 5.2.2061035
 mac address   : 00:1b:8b:54:6e:e9
 antenna level : Current 2 [Max 6]
 running state : ESTABLISHED(IDLE)
 running mode  : Adapter
 detect status : FastEthernet0.0 link up
```

← 運用ステータスを確認します。

メモ　運用ステータスに表示される主要なエラーは以下の通りです。エラー表示を確認し、対処をお願いします。

主要エラー表示	対処方法
ERROR（AUTH）	WiMAXの認証処理にエラーがあります。 本製品の電源を投入しなおすか、コマンドによる再起動を行ってください。またはコマンドによるWiMAX接続の初期化を行ってください。
ERROR（ROM）	ご利用のデータ通信端末のサービス加入手続きが完了していません。 WiMAXサービス提供元に、サービス加入手続きが完了しているかをお問い合わせしてください。
ESTABLISHED（DHCP WAIT）	DHCP処理が完了していません。 アダプタモードでお使いになっている場合は、配下ルータにDHCPクライアントが正しく設定されているかを確認ください。 ルータモードでお使いになっている場合、本製品の電源を投入しなおすか、コマンドによる再起動を行ってください。またはコマンドによるWiMAX接続の初期化を行ってください。
UNKNOWN	販売元にご相談ください。

■モバイル通信が不調のときは

本製品は、モバイル通信において異常を検出すると、通信の復旧をはかるために自動的に装置を再起動する機能があります。モバイル通信の異常とは、以下のような状態をさします。

- データ通信端末が動作不調になった場合
- 基地局との通信が不調になった場合

WA1020では、通信が不調になった際に再起動が行われるように設定されています。ご使用の環境に応じて、データ通信端末が不調になった際に再起動が行われるように追加設定することもできます。

WA1510、WA1511、WA2020、WA2021では、工場出荷時に本機能は無効になっています。本機能を常時有効にするためには、CLIから手動で有効設定を行ってください。バックアップ時のみ有効にしたい場合は、5章のネットワーク設定例「ネットワークモニタ機能設定例」を参照して、設定を行ってください。

本機能による再起動が発生した場合は、エラーログに「system reboot(要因)」と示す以下のようなログが残ります。

```
WA1020(config)#
WA1020(config)# show error-log [Enter]
:
:

-----------------------------
[2011-06-01 11:59:36 FAULT STRING]
system reboot (Authentication error).

-----------------------------
[2011-06-01 11:59:36 DUMP SYSLOG]
 :
 :
2011-06-01 11:59:36 WIMAX.INFO Send disconnect message (SYNCDOWN:14)
2011-06-01 11:59:36 WIMAX.ERR system reboot (Authentication error).

:
:


WA1020(config)#
```

メモ　H/WやSWの関連する事象でもエラーログが記録されます。上記の様なエラーログが再発する場合や、別のメッセージが記録されている場合は、本章の「装置設定や動作を問い合わせたい」をご確認になり、販売元へご相談ねがいます。

■内蔵モジュールで WAN に接続できないときは

WA1511 は、モバイル通信において、内蔵モジュールを使用します。本モジュールは、工場出荷時に SIM カードを内蔵していません。ご用意いただいた SIM カードを含め、以下を確認してください。

1） アンテナが正しく2本接続されているか。
背面のコネクタの接続とアンテナの向き（交差していないか、金属にふれていないか、オプション品は縦に取り付けられているか）や断線等をご確認ねがいます。

2） SIMカードが内蔵モジュールの仕様(通信事業者/契約等)とあっているか。
販売元にWA1511が、どの通信事業者に対応したものであるかをご確認いただき、対応しているSIMカードであることを確認します。

3） SIMカードが正しく接続されているか。
(差し込み口の位置、差し込み方向、切欠き方向)
SIMカードが正しく装着されていることを確認します。(SIMカードの接続と抜去は、電源OFFが必要です。)

4） show mobile status にて内蔵モジュールが認識されているか
show mobile statusにて、エラーなく内蔵モジュールが動作していることを確認します。内蔵モジュールが正常に動作しエラー等がない場合は、本項の最初のページの内容からご確認ねがいます。

SIM ERROR等が表示されている場合、SIMカードの接続のやり直しを実施してください。SIMカードがモジュールに対応しているにもかかわらず、SIM ERRORが解消しない場合は、販売元にご連絡ください。

また、内蔵モジュールが認識されない場合は、販売元にご連絡ください。

ANTENNA LEVEL ZERO表示が出ている場合は、アンテナが適切に接続されているか、電波状態をご確認ねがいます。

メモ　内蔵モジュールのリカバリ等チェックを定期的に行う設定をしている場合、モジュールが表示されず、認識されていない様に見える場合がありますので、数回show mobile statusを確認してください。

5） PIN認証で3回失敗し、ロック状態になっていないか
SIM LOCKEDが表示されている場合は、PINロックがかかっている状態です。
WA1511内蔵モジュールでは、PINロック解除コマンドでロック解除します。
解除方法は、4-1章「データ通信を始める前に」の「WA1511内蔵モジュールのPINロック解除手順」をご参照お願いいたします。

PPPoEでWANに接続できないときは

PPPoE機能はWA1510、WA1511、WA2020、WA2021で利用可能です。

ローカルコンソールから、設定の確認、WANの状態を確認します。PPPランプでも状況確認できます。

1） 契約しているプロバイダの契約内容を確認し、ユーザIDやパスワードの設定内容が正しいか確認してください。

2） WANに接続している物理インタフェースがリンク確立しているか確認してください。物理インタフェースがリンク確立していないとPPPoEでの接続はできません。

3） 物理インタフェースにPPPoEインタフェースが割り当てられているか確認してください。

4） show interfaces PPPoEx (x:設定したインタフェース番号)でエラー状態を確認してください。

```
WA1020(config)# show interfaces PPPoE0
Interface PPPoE0 is up
  IP address
    (local) 183.72.31.60 -> (remote) 110.158.22.137
  MTU size is 1492 bytes
  PPPoE: client
    Bind interface GigaEthernet0.0
    session id 0xe41
    state : SESSION
  PPP:
    LCPMGR: NETWORK
    LCP   : opened
    IPCP  : opened          ←
  FAIL-CODE: NONE              エラー状態を確認します。
```

メモ　表示される主要なエラーは以下の通りです。エラー表示を確認し、対処をお願いします。

主要エラー表示	対処方法
ADMIN_IPCP_DISCONNECT	要求時接続の設定になっており、idle-timer が満了したことにより切断状態となっています。常時接続の設定に変更するか、LAN配下のパソコンから通信を開始してください。
PADI_TIMEOUT PADR_TIMEOUT LCP_FAIL LCP_TIMEOUT AUTH_TIMEOUT IPCP_TIMEOUT	プロバイダと接続できません。契約プロバイダにて障害が発生している可能性があります。 契約プロバイダに障害状況を確認してください。
AUTH_FAIL	認証エラーが発生しています。契約内容を確認し、IDとパスワードが正しいか確認してください。 また、認証方式が正しいか確認してください。
UNKNOWN	販売元にご相談ください。

無線LANがつながらないときには

無線LANアクセスポイント機能はWA2021のみ利用可能です。

ローカルコンソールから、WA2021設定、無線LANインタフェースの状態を確認します。
WA2021およびWA100-APのランプでも状況確認できます。

1） WA100-AP無線LANカードが、WA2021に正しく接続されていることを確認してください。WA2021正面のPCランプやWA100-APのPWR/ACTランプでも確認できます。

2） ネットワーク名（SSID）および暗号化キー設定が、WA2021と無線LAN子機で一致しているかを確認してください。

3） IEEE802.11nは、IEEE802.11b/g/nが混在する環境では動作が不安定になる場合があります。IEEE802.11nで動作が安定しない場合は、動作モードをIEEE802.11gまたはIEEE802.11bに変更してください。

4） WA2021の設置場所や、無線LAN子機との距離を変えてみてください。

5） show wireless コマンドで無線LAN子機の接続状態を確認してください

```
WA2021# show wireless stations
Interface WirelessEthernet0.0 stations information. (Associated Stations : 1)
  Station MAC Address: 8c:7b:9d:78:f9:bb
    essid                          : WA2021-SSID-1
    phy mode                       : 802.11n
    Association ID                 : 49153
    fastframe                      : disable
    compression                    : disable
    authmode                       : wpa2
    cipher                         : aes-ccm
    unicast-key                    : ********************************
    group-key                   [0]:
    group-key                   [1]: ********************************
    group-key                   [2]: ********************************
    group-key                   [3]: ********************************
    channel                        : 5
    TXRATE                         : 51 [Mbps]
    RSSI                           : 55
    IDLE                           : 15
    TXSEQ                          : 9
    RXSEQ                          : 800
    RXPOWER                        : 32
    ERP                            : 0x00
    STATE                          : AUTH QOS ERP HT PWR_MGT
    CAPS                           : ESS PRIVACY SHORT-PRE SHORT-SLOTTIME
    ATHCAPS                        :
    Extend-IE Information
       RSN<30140100000fac020100000fac040100000fac020c00>
       WME<dd070050f202000100>

Interface WirelessEthernet0.1 stations information. (Associated Stations : 0)
Interface WirelessEthernet0.2 stations information. (Associated Stations : 0)
Interface WirelessEthernet0.3 stations information. (Associated Stations : 0)
```

接続子機数

```
WA2021# show wireless access-history
Interface WirelessEthernet0.0 access history
  Mac Address
    xx:27:xx:9c:xx:01
    00:xx:9d:xx:02:xx
```

過去に接続した子機の MAC アドレス（最大 50 件）

自動的に再起動したときは

本製品の障害により自動的に再起動した場合には、以下の情報が必要となります。

販売元にご連絡いただく前に、以下の情報をあらかじめご準備いただけるようお願い致します。

1） 障害発生時の状況

ネットワーク工事や、端末の追加など、何らかの工事による影響を確認してください。

2）製品前面LEDの状態

製品前面LEDの表示が正常であるか確認してください。

3）ネットワーク構成

本製品を使用している全体のネットワーク構成（ネットワーク機器のIPアドレスや製品名、使用回線など）

4）設定情報と障害情報

再起動直前の障害情報が自動的にフラッシュメモリ内に保存されます。
このデータを次の「解析情報の収集方法」により収集してください。
このような自動再起動が発生した場合には、障害解析のためにお客様の設定情報や障害情報が必要となります。これは、ソフトウェアの障害解析に必ず必要となる情報で、この情報が無いと障害解析が困難になります。

装置設定や動作を問い合わせたい

障害解析などのため、装置の設定状態やイベント情報を収集する場合は、show technical-support コマンドを実行することで収集可能です。解析情報を収集し、販売元へご相談ください。

```
WA1020# show technical-support

---------------------- [ show clock ] --------------------
Thu  1 January 2009 00:08:08
uptime is 0 days 0 hours 0 minutes 35 secs.

---------------------- [ show version ] --------------------
Copyright (c) NEC Platforms, Ltd. 2009-2010 All rights reserved.
Copyright (c) 1996-2004
   The NetBSD Foundation, Inc.  All rights reserved.
Copyright (c) 1982, 1986, 1989, 1991, 1993
   The Regents of the University of California.  All rights reserved.
Operating System Software : version 3.1.0
Compiled:  Fri Oct  1 09:16:36 JST 2010

Serial Number: 11*******

Hardware Revision: 2.0
uptime is 0 days 0 hours 0 minutes 35 secs.
memory size is 134217728 [byte]

---------------------- [ show running-config ] --------------------
! Product: WA1020
! Version: 3.1.0
! Date: 2009/01/01 00:08:08
!
syslog enable
syslog function all debug
!
hostname WA1020
!
username admin password hash $1$G1AuQIZG$5tO0hWbhinUMCmYk61zbD/
administrator
!
no wireless-adapter enable
!
!
interface FastEthernet0.0
  ip address 192.168.1.200/24
  ip dhcp-server binding default
  no shutdown
!
interface Serial0
  ip address ipcp
  ip tcp adjust-mss auto
  ip napt enable
  ip napt reserve esp
  ip napt reserve udp 500
  mobile number *99***CID#
  auto-connect
  shutdown
!
!
    (以下、省略)

WA1020#
```

8
仕様

諸元

【WA1020 ハードウェア】

項目		仕様
外形寸法		135mm（W）×160mm（D）×33mm（H）以下 （突起物を除く）
重量		約 0.4kg（AC アダプタ含む）
LAN 側 インタフェース （FastEthernet）	物理インタフェース	8 ピンモジュラージャック（RJ-45）
	ポート数	1 ポート
	規格	100BASE-TX/10BASE-T ※1、 Auto-MDI/MDIX、IEEE802.3u/802.3
	伝送速度	100Mbps/10Mbps
	全二重／半二重	オートネゴシエーション
WAN 側 インタフェース	PC カードスロット	1 スロット （TypeI/II、PCMCIA（16bit）／CardBus（32bit）共用）
	USB ポート	1 ポート（USB2.0 LS/FS/HS モード対応）※2
コンソールポート		RS232C（RJ-45）
表示部 （前面 LED）	状態表示 LED	PWR、STAT、PPP、MODE、Mobile（PC）、Mobile（USB）
	FE0	速度状態、LINK 状態、データ送受信時点滅
スイッチ／端子類	電源端子	AC アダプタ抜き差し
	初期化スイッチ	装置初期化
電源		AC100V±10%　50/60Hz（AC アダプタ）
消費電力		約 10VA（約 4W）※3
設置方法		横置き、縦置き、壁掛け
動作保証範囲		温度　0～45℃　湿度　90%以下（非結露）※4
対応法令及び品質規格		VCCI クラス B、RoHS 対応

※1　本製品を快適にお使いになるためには、100BASE-TX、100Mbps の方式での接続を推奨します。また LAN ケーブルは CAT5 の使用をお奨めします。

※2　HS モードは、製品レビジョン 2.0 以降のみのサポートです。また USB ハブや USB 延長ケーブルによる接続はしないでください。

※3　本体のみの場合の消費電力です。

※4　データ通信端末を接続してご利用になる場合には、データ通信端末にて指定されている環境条件範囲内でのご利用を推奨致します。

【WA1510／WA1511 ハードウェア】

項目		仕様
外形寸法		160mm（W）×135mm（D）×33mm（H） （突起物を除く）
重量		WA1510 約 0.6kg（AC アダプタ含む） WA1511 約 0.75kg（AC アダプタ、アンテナ含む）
WAN 側 インタフェース GE0 (GigabitEthernet)	物理インタフェース	8 ピンモジュラージャック(RJ-45)
	ポート数	1 ポート
	規格	1000BASE-T/100BASE-TX/10BASE-T ※1 Auto-MDI/MDIX IEEE802.3u/802.3
	伝送速度	1Gbps/100Mbps/10Mbps
	全二重／半二重	オートネゴシエーション
	その他	・速度、duplex 設定は以下の組み合わせ (auto,1000Mfull,100Mfull,100Mhalf,10Mfull,10Mhalf)
LAN 側 インタフェース GE1 (GigabitEthernet)	物理インタフェース	8 ピンモジュラージャック(RJ-45)
	ポート数	1 ポート
	規格	1000BASE-T/100BASE-TX/10BASE-T ※1 Auto-MDI/MDIX IEEE802.3u/802.3
	伝送速度	1Gbps/100Mbps/10Mbps ※1
	全二重／半二重	オートネゴシエーション
	その他	・速度、duplex 設定は以下の組み合わせ (auto,1000Mfull,100Mfull,100Mhalf,10Mfull,10Mhalf)
WAN 側 インタフェース	USB ポート	1 ポート（USB2.0、LS/FS/HS モード対応）※2
アンテナ端子 (WA1511 のみ)		SMA-J × 2 ポート
コンソールポート		RS232C（RJ-45）
表示部 （前面ランプ）	状態表示ランプ	PWR、STAT、PPP、VPN、BAK、Mobile、MODE
	GE0/GE1	速度状態、LINK 状態、データ送受信時点滅
スイッチ／端子類	電源端子	AC アダプタ抜き差し
	初期化スイッチ (INIT)	装置初期化
電源		AC100V±10% 50/60Hz（AC アダプタ）
消費電力		WA1510 約 5.5W ※3 WA1511 約 7.2W ※4(最大 8.5W)
設置方法		横置き、縦置き、壁掛け
動作保証範囲		温度 0～45℃ 湿度 90%以下（非結露）※5
対応法令及び品質規格		VCCI クラス B、RoHS 対応

※1 本製品を快適にお使いになるためには、1000BASE-T、1000Mbps もしくは 100BASE-TX、100Mbps の方式での接続を推奨します。また LAN ケーブルは CAT5e の使用をお奨めします。
※2 USB ハブや USB 延長ケーブルによる接続はしないでください。
WAN 側インタフェースと使用できるのは、WA1510 のみです。
※3 本体のみの場合の消費電力です。利用するデータ通信端末によって消費電力は変動します。
※4 HSPA 無線通信を行っている場合の平均消費電力です。
※5 データ通信端末を接続してご利用になる場合には、接続する端末にて指定されている環境条件範囲内でご使用ください。

【WA2020／WA2021 ハードウェア】

項目		仕様
外形寸法		174mm（W）×195mm（D）×40mm（H） （突起物を除く）
重量		約 1.1kg（AC アダプタ含む）
WAN 側 インタフェース GE0 (GigabitEthernet)	物理インタフェース	8 ピンモジュラージャック(RJ-45)
	ポート数	1 ポート
	規格	1000BASE-T/100BASE-TX/10BASE-T ※1 (Auto-MDI/MDIX 対応) IEEE802.3u/802.3
	伝送速度	1Gbps/100Mbps/10Mbps
	全二重／半二重	オートネゴシエーション
	その他	・速度、duplex 設定は以下の組み合わせ (auto,1000Mfull,100Mfull,100Mhalf,10Mfull,10Mhalf) ・MDI 設定(固定/auto)
LAN 側 インタフェース GE1(LAN1-4) (GigabitEthernet)	物理インタフェース	8 ピンモジュラージャック(RJ-45)
	ポート数	4 ポート(SW-HUB)
	規格	1000BASE-T/100BASE-TX/10BASE-T ※1 (Auto-MDI/MDIX 対応) IEEE802.3u/802.3
	全二重／半二重	オートネゴシエーション
	その他	・速度、duplex 設定は以下の組み合わせ (auto,1000Mfull,100Mfull,100Mhalf,10Mfull,10Mhalf) ・MDI 設定(固定/auto)。 ※ポート単位は不可
WAN 側 インタフェース	PC カードスロット	1 スロット ※5 （TypeI/II、PCMCIA（16bit）／CardBus（32bit）共用）
	USB ポート	2 ポート（USB2.0、LS/FS/HS モード対応）※2
コンソールポート		RS232C（RJ-45）
表示部 （前面ランプ）	状態表示ランプ	PWR、STAT、PPP、VPN、BAK、USB、PC
	GE0/GE1	速度状態、LINK 状態、データ送受信時点滅
スイッチ／端子類	電源端子	AC アダプタ抜き差し
	初期化スイッチ (INIT)	装置初期化
電源		AC100V±10% 50/60Hz（AC アダプタ）
消費電力		約 15VA（約 8W）※3
設置方法		横置き、縦置き
動作保証範囲		温度 0～45℃ 湿度 90％以下（非結露）※4
対応法令及び品質規格		VCCI クラス B、RoHS 対応

※1 本製品を快適にお使いになるためには、1000BASE-T、1000Mbps もしくは 100BASE-TX、100Mbps の方式での接続を推奨します。また LAN ケーブルは CAT5e の使用をお奨めします。

※2 USB ハブや USB 延長ケーブルによる接続はしないでください。

※3 本体のみの場合の消費電力です。

※4 データ通信端末もしくは無線 LAN カード WA100-AP を接続してご利用になる場合には、接続する端末、カードにて指定されている環境条件範囲内でご使用ください。

※5 WA2021 では、PCMCIA(16bit)タイプの PC カードは使用できません。

【ソフトウェア】

<table>
<tr><th colspan="2">項目</th><th colspan="4">仕様</th></tr>
<tr><td colspan="2">製品名</td><td>WA1020</td><td>WA1510/WA1511</td><td>WA2020</td><td>WA2021</td></tr>
<tr><td rowspan="4">共通機能</td><td>ルータ機能</td><td colspan="4">スタティックルーティング、ポリシールーティング</td></tr>
<tr><td>対応データ通信端末</td><td colspan="4">下記 URL 参照
http://jpn.nec.com/univerge/wa/</td></tr>
<tr><td>運用監視機能</td><td colspan="4">SSH サーバ機能、TELNET サーバ機能、TFTP クライアント機能、FTP クライアント機能、SNMP エージェント（SNMPv2、標準 MIB、プライベート MIB）機能、SYSLOG 機能、デバッグ機能、ping 機能、Traceroute 機能、SNTP クライアント機能、データ通信端末 PIN 認証機能、PIN ロック解除機能(WA1511 のみ)、データ通信端末リカバリー機能、切断スケジュール機能、メール送信機能、N2502 端末 IP 着信サービス対応 ※1、自動バージョンアップ機能、自動コンフィグファイル更新機能、電波サーベイ機能、パケットダンプ機能、Web-GUI 機能、USB ストレージ機能、課金パケット計測機能、トラフィック流量表示機能</td></tr>
<tr><td>その他</td><td>PPP クライアント、タグ VLAN 機能</td><td>PPP クライアント(WA1510)、
PPPoE クライアント、
タグ VLAN 機能</td><td colspan="2">PPP クライアント、PPPoE クライアント、タグ VLAN 機能、
ポート VLAN 機能、
storm-suppression 機能</td></tr>
<tr><td colspan="2">無線 LAN 機能</td><td colspan="3">―</td><td>無線 LAN AP モード</td></tr>
<tr><td colspan="2">動作モード</td><td>アダプタモード、ルータモード</td><td colspan="3">ルータモード</td></tr>
<tr><td rowspan="2">アダプタモード</td><td>アダプタ接続</td><td>PPPoE サーバ、PPP ブリッジ（プロキシ）機能、WiMAX ブリッジ（プロキシ）機能、WiMAX オンデマンド機能</td><td colspan="3">―</td></tr>
<tr><td>障害検知</td><td>リンクパススルー機能</td><td colspan="3">―</td></tr>
<tr><td rowspan="2">ルータモード</td><td>ルータ機能</td><td colspan="4">DHCP サーバ機能、DHCP クライアント機能、DHCP リレーエージェント機能、アドレス変換機能（NAT/NAPT）、プロキシ DNS 機能、Dynamic DNS 機能、IPSec 機能、EtherIP 機能、L2TPv3 機能、ネットワークモニタ機能、VRRP 機能、WiMAX オンデマンド機能※2、proxy arp 機能</td></tr>
<tr><td>セキュリティ</td><td colspan="4">IP パケットフィルタ機能、MAC フィルタ機能、ダイナミックフィルタ機能、SSH/telnet アクセスフィルタ機能</td></tr>
</table>

※1　WA1510/WA1511/WA2021 は、N2502 端末 IP 着信サービスをサポートしておりません。

※2　WA1510/WA1511 は、WiMAX データ通信端末及び WiMAX オンデマンド機能をサポートしておりません。

【IPsec】

項目			仕様	
製品名			WA1020	WA1510/WA1511 WA2020/WA2021
IPsec	セッション数		2 対地	8 対地
	モード		トンネルモード、トランスポートモード	
	セキュリティ プロトコル		ESP	
	サポートアルゴリズム	暗号化	DES、3DES、AES-128、AES-192、AES-256、Null	
		認証	HMAC-MD5-96、HMAC-SHA-1-96、HMAC-SHA-2-256	
	鍵交換方式		自動鍵（鍵交換プロトコル：IKEv1）	
	SA ライフタイム		時間指定、時間/データ量指定	
	Rekey		有効（トラフィックあり時、Rekey）／無効、常時接続	
	Peer 設定		IP アドレスまたは FQDN	
IKE	交換タイプ		メインモード、アグレッシブモード	
	認証方式		事前鍵共有方式（Pre-Shared Key）	
	サポートアルゴリズム	暗号化	DES、3DES、AES-128、AES-192、AES-256	
		認証	HMAC-MD5、HMAC-SHA-1、HMAC-SHA-2-256	
	DH グループ		768bit（group1）、1024bit（group2）、1536bit（group5）、2048bit（group14）	
	IKE ID 設定		Key-id、address、FQDN、USER_FQDN	
その他	IKE SA と IPsec SA の依存関係		Continuous-channel SA 型	
	TCP mss 調整機能		自動/固定設定	
	NAPT 同時動作		IPsec 利用時に NAPT による外部接続の同時動作可能	
	フィルタリング		IPsec トンネルインタフェースにて制御可能	
	オプション		Initial-Contact、Keep-Alive（DPD 方式）、commit-bit	
	Inner-NAT/NAPT 機能		IPsec トンネル通過の通信に対する NAT/NAPT 変換	
	NAT トラバーサル		対応	

【WA1511 添付品：L 型直付けアンテナ】

項目	仕様
外形寸法	162mm（W）×26mm（D）×15mm（H）以下 （コネクタ部除く）
コネクタ	SMA-P
使用周波数	800MHz 帯/1.5GHz 帯/2GHz 帯
設置方法	本体直付け(L 型)
動作保証範囲	温度　-5～50℃
対応法令及び品質規格	RoHS 対応

【製品オプション(別売)：無線 LAN カード】

<table>
<tr><th colspan="2">項目</th><th colspan="2">仕様</th></tr>
<tr><td rowspan="12">無線 LAN
ポート</td><td>端末インタフェース</td><td colspan="2">ExpressCard/34 (PCI Express) 準拠</td></tr>
<tr><td rowspan="3">IEEE802.11b</td><td>周波数帯／チャネル</td><td>2.4GHz 帯 (2,400～2,484MHz) ／ 1～13ch</td></tr>
<tr><td>伝送方式</td><td>DS-SS (スペクトラム直接拡散) 方式</td></tr>
<tr><td>伝送速度 (※1)</td><td>11/5.5/2/1Mbps (自動切換)</td></tr>
<tr><td rowspan="3">IEEE802.11g</td><td>周波数帯／チャネル</td><td>2.4GHz 帯 (2,400～2,484MHz) ／ 1～13ch</td></tr>
<tr><td>伝送方式</td><td>OFDM (直交周波数分割多重) 方式</td></tr>
<tr><td>伝送速度 (※1)</td><td>54/48/36/24/18/12/9/6Mbps (自動切換)</td></tr>
<tr><td rowspan="3">IEEE802.11n</td><td>周波数帯／チャネル</td><td>2.4GHz 帯 (2,400～2,484MHz) ／ 1～13ch</td></tr>
<tr><td>伝送方式</td><td>OFDM (直交周波数分割多重) 方式
MIMO (空間多重) 方式</td></tr>
<tr><td>伝送速度 (※1)</td><td>[HT20]
144.4/130/117/104/78/72.2/65/58.5/52/
39/26/19.5/13/6.5Mbps
[HT40]
300/270/243/216/162/150/135/121.5/
108/81/54/40.5/27/13.5Mbps (自動切換)</td></tr>
<tr><td>アンテナ</td><td colspan="2">MIMO 送信 2×受信 2</td></tr>
<tr><td>セキュリティ</td><td colspan="2">WEP(152/128/64bit)
WPA-PSK(TKIP/AES)、WPA2-PSK(TKIP/AES)</td></tr>
<tr><td colspan="2">LED 表示</td><td colspan="2">PWR (緑) 1 個、ACT (緑) 1 個</td></tr>
<tr><td colspan="2">動作環境</td><td colspan="2">温度：0～40℃　湿度：20～85% (非結露)</td></tr>
<tr><td colspan="2">外形寸法</td><td colspan="2">約 34 (W) × 5 (D) × 112 (H) mm (突起部分を除く)</td></tr>
<tr><td colspan="2">電源</td><td colspan="2">DC 3.3 V</td></tr>
<tr><td colspan="2">消費電力</td><td colspan="2">最大 2.2 W</td></tr>
<tr><td colspan="2">質量</td><td colspan="2">約 0.03 kg</td></tr>
<tr><td colspan="2">電磁妨害波規格</td><td colspan="2">VCCI クラス B</td></tr>
</table>

※1　無線 LAN の規格であり、実際のデータ転送速度を示すものではありません。

【製品オプション(別売)：PC カードアダプタ】

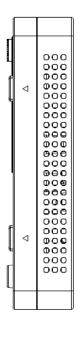
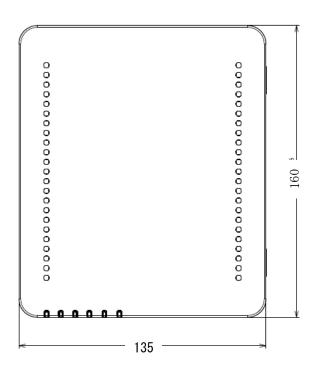
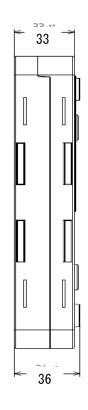
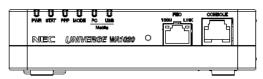
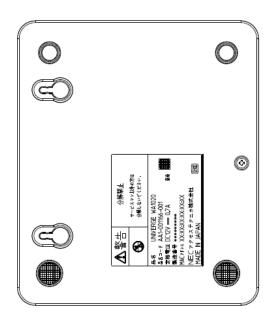
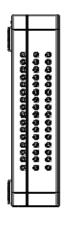
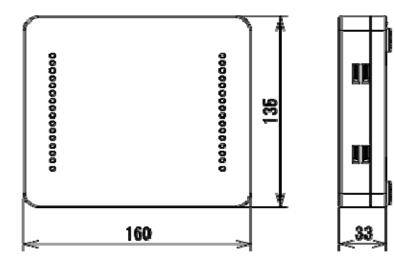
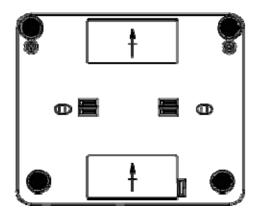
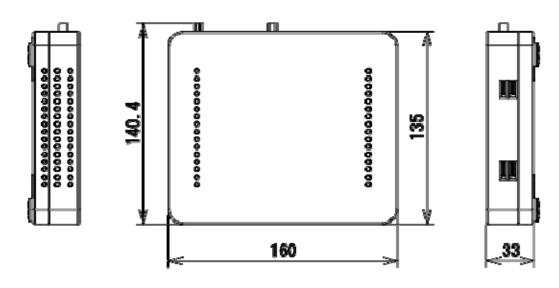
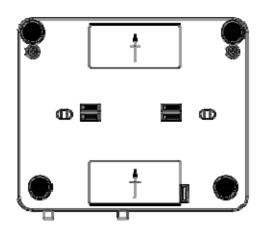
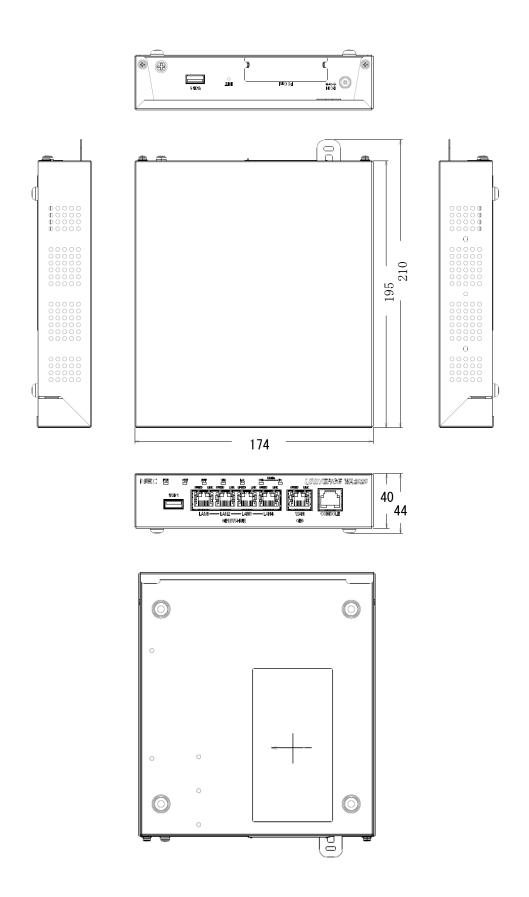
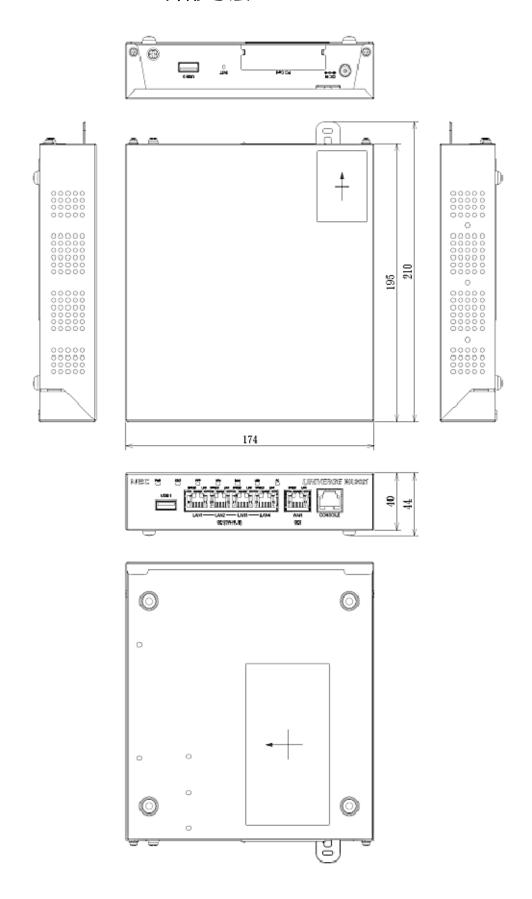
項目	仕様
PC カード (CardBus) コネクタ	PC Card Standard (CardBus) Type II 準拠
ExpressCard/34(PCI Express)コネクタ	ExpressCard/34(PCI Express)準拠
動作環境	温度：0～40℃　湿度：20～85% (非結露)
外形寸法	約 54(W) × 5 (D) × 112.6 (H) mm (突起部分を除く)
電源	DC 3.3 V
消費電力	最大 0.7 W
質量	約 0.03 kg
電磁妨害波規格	VCCI クラス B

【製品オプション(別売)：延長アンテナ 2.5m/5m】

項目	仕様
外形寸法	110mm（W）×40mm（D）×25mm（H）以下 （アンテナ部のみ）
重量	約 90g（延長アンテナ 2.5m）約 120g（延長アンテナ 5m）
コネクタ	SMA-P
ケーブル長	2.5m（延長アンテナ 2.5m）、5m（延長アンテナ 5m）
使用周波数	800MHz 帯/1.5GHz 帯/2GHz 帯
設置方法	ねじ止め、両面テープ、ラバーマグネット
動作保証範囲	温度　-20～90℃　(ネジ止め) -20～80℃(両面テープ、ラバーマグネット使用時)
対応法令及び品質規格	RoHS 対応

【製品オプション(別売)：USB メモリ（T-512）】

項目	仕様
外形寸法	61mm（W）×19.4mm（D）×8.6mm（H）以下
容量	512MB
読み書き性能	Read: 16 MB/sec (max.), Write: 8 MB/sec (max.)
USB 仕様	USB2.0、LS/FS/HS モード対応
動作保証範囲	温度　0～70℃
対応法令及び品質規格	RoHS 対応

■UNIVERGE WA1020外形寸法

■UNIVERGE WA1510外形寸法

■UNIVERGE WA1511外形寸法

■UNIVERGE WA2020外形寸法

■UNIVERGE WA2021外形寸法

インタフェース仕様

■コンソールポートコネクタ

本製品側のコンソールコネクタは、8ピンモジュラコネクタ（RJ-45）です。ローカルコンソール(PC等)を接続するときは、添付のRS-232Cストレートケーブルをご使用ください。

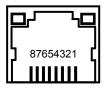
形状

ピンアサイン

ピン番号	信号名
1	―
2	DSR（DR）
3	RxD（RD）
4	SG
5	SG
6	TxD（SD）
7	DTR（ER）
8	―

■**FE0　10/100BASE-TX** ポート・コネクタ**(WA1020)**

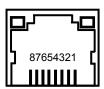
インタフェースコネクタは、8ピンモジュラコネクタ（RJ-45）にて提供します。

形状

ピンアサイン

ピン番号	信号名
1	Transmit＋
2	Transmit－
3	Receive＋
4	―
5	―
6	Receive－
7	―
8	―

■GE0　10/100/1000BASE-TX ポート・コネクタ(WA2020／WA2021)
GE0/GE1　10/100/1000BASE-TX ポート・コネクタ(WA1510／WA1511)

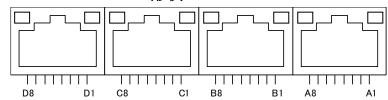
インタフェースコネクタは、8ピンモジュラコネクタ（RJ-45）にて提供します。

形状

ピンアサイン（**MDI**）

ピン番号	1000BaseT時信号名	100/10TX時信号名
1	BI_D_A+	Transmit＋
2	BI_D_A-	Transmit－
3	BI_D_B+	Receive＋
4	BI_D_C+	－
5	BI_D_C-	－
6	BI_D_B-	Receive－
7	BI_D_D+	－
8	BI_D_D-	－

■GE1　10/100/1000BASE-TX ポート・コネクタ(WA2020／WA2021)

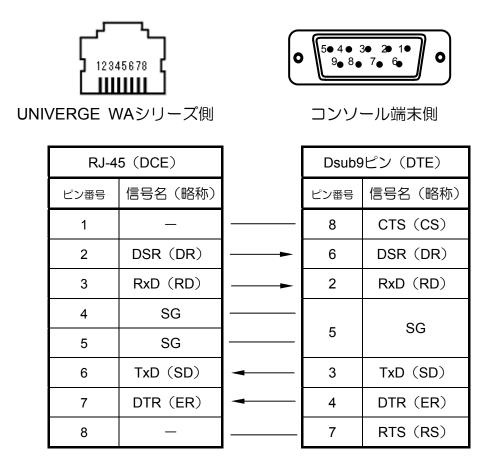
インタフェースコネクタは、4連、8ピンモジュラコネクタ（RJ-45）にて提供します。

形状

ピンアサイン（**MDI-X**）

ピン番号	1000BaseT時信号名	100/10TX時信号名
1	BI_D_B+	Receive＋
2	BI_D_B-	Receive－
3	BI_D_A+	Transmit＋
4	BI_D_D+	－
5	BI_D_D-	－
6	BI_D_A-	Transmit－
7	BI_D_C+	－
8	BI_D_C-	－

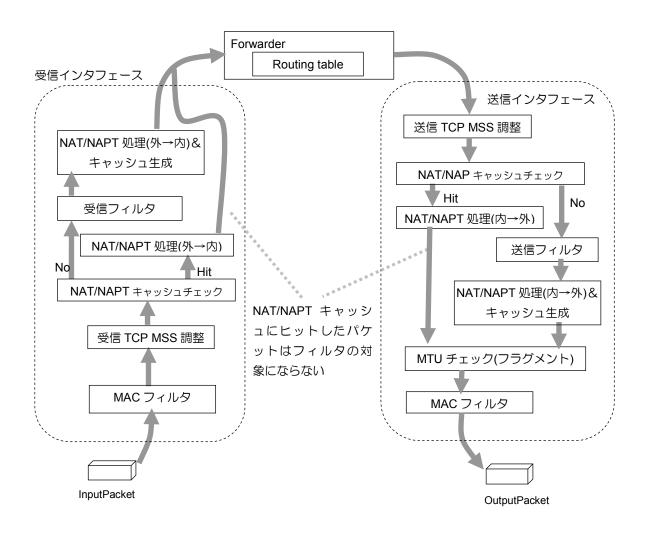
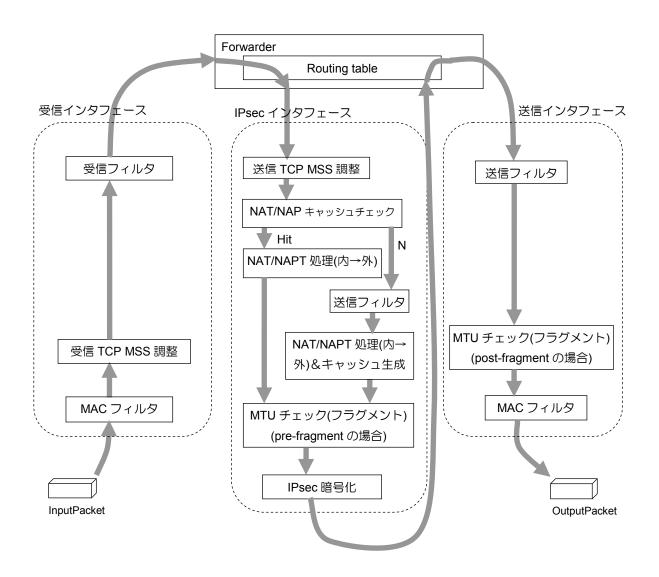
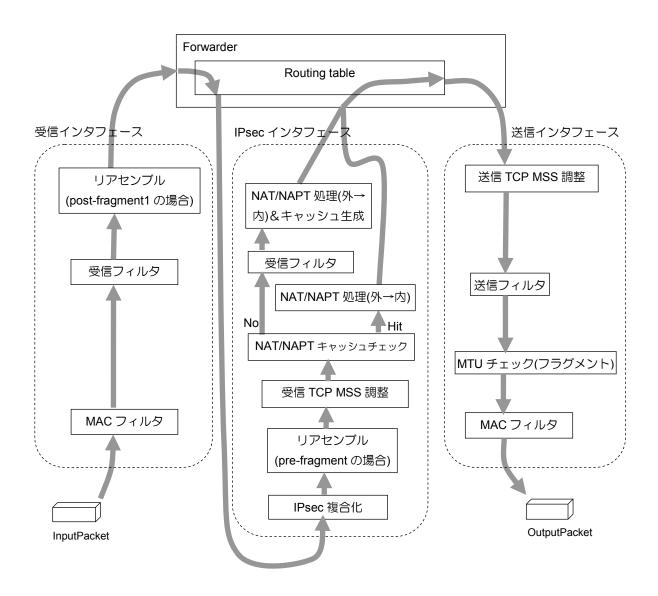
■コンソールケーブル両端コネクタ

添付のRS-232Cコンソールケーブル（RJ45―Dsub9ピン）コネクタ間の結線は以下となっています。

RJ-45（DCE）			Dsub9ピン（DTE）	
ピン番号	信号名（略称）		ピン番号	信号名（略称）
1	―	――	8	CTS（CS）
2	DSR（DR）	→	6	DSR（DR）
3	RxD（RD）	→	2	RxD（RD）
4	SG	――	5	SG
5	SG	――	5	SG
6	TxD（SD）	←	3	TxD（SD）
7	DTR（ER）	←	4	DTR（ER）
8	―	――	7	RTS（RS）

＜付録＞

パケット評価フロー

WAシリーズの IPv4 Forwarder 配下のパケットの評価順を説明します。

- IPv4パケット評価フロー

• IPsec（トンネルモード）送信時の評価フロー

- IPsec（トンネルモード）受信時の評価フロー

VLAN機能の注意点

VLAN機能を使用する上での注意点と､その他ルータ機能との連携に関する注意点を説明します。

[VLAN機能を使用する上での注意点]

ポートVLANとタグVLANを設定する場合、以下の点に注意する必要があります。

• タグVLAN

項目	内容
使用可能インタフェース	WA1020：FE0.0 WA1510/WA1511：GE0.0、GE1.0 WA2020：GE0.0、GE1.0 WA2021：GE0.0、GE1.0
SW-HUB ポート間のタグVLANフレームの転送	vlan-typeコマンドでポート指定を行わない場合、各スイッチポートにて受信したタグVLANフレームはその他のスイッチポートに転送されます。
ポートVLANとの併用	同一のベースインタフェースで、ポートVLANとの併用はできません。
タグVLANポート指定	WA2020、WA2021のGE1.0のみ利用可能です。
ポート指定/無指定の混在	vlan-typeコマンドで1つでもポート指定を行った場合、全てのvlan-typeコマンドにてポート指定が必要です。 interface GigaEthernet1.0 vlan-type tagged VLAN0 tag-id 123 port 1 vlan-type tagged VLAN1 tag-id 456（設定できません）
ポート指定時の未指定ポート使用	vlan-typeコマンドで1つでもポート指定を行った場合、未指定のポートは利用できません。（ただし未指定のスイッチポートはLink-Downしません)
ポート指定時のベースインタフェース使用	vlan-typeコマンドで1つでもポート指定を行った場合、ベースインタフェースは利用できません。
複数VLANインタフェースへの同一タグID指定	同一のベースインタフェースにて、同一のタグVLAN ID（VID）を複数のVLANインタフェースに割り当てることは出来ません。 interface GigaEthernet1.0 vlan-type tagged VLAN0 tag-id 123 vlan-type tagged VLAN1 tag-id 123（設定できません）
異なるベースインタフェースへの同一タグID指定	異なるベースインタフェースにて、同一のタグVLAN ID（VID）を複数のVLANインタフェースに割り当てることは可能です。

項目	内容
	interface GigaEthernet0.0 vlan-type tagged VLAN0 tag-id 123 interface GigaEthernet1.0 vlan-type tagged VLAN2 tag-id 123
異なるベースインタフェース間のL2転送	異なるベースインタフェースのVLANインタフェースに、同一のタグVLAN ID（VID）を設定しても同じブロードキャストドメインとはなりません。VLANインタフェース間は、ルーティング動作です。
二重タグ指定(QinQ)	タグVLANインタフェースで二重タグを利用することは出来ません。
設定後の再起動の要否	タグVLAN設定時は即時反映が可能です。 ただし、vlan-typeコマンドでポート指定を行った場合は再起動が必要です。（WA2020、WA2021）

• ポートVLAN

項目	内容
使用可能インタフェース	WA2020：GE1.0 WA2021：GE1.0
タグVLANとの同時使用	同一のベースインタフェースで、ポートVLANとの併用はできません。
ベースインタフェースの使用	ポートVLANを利用する場合、ベースインタフェースは利用することが出来ません。
SW-HUBポートのグルーピング	複数のSW-HUBポートを1つのポートVLANインタフェースに割り当てることは出来ません。
未指定ポートの使用	vlan-typeコマンドで1つでもポートVALN指定を行った場合、未指定のポートは利用できません。（ただし未指定のスイッチポートはLink-Downしません)
タグ付きフレームの対応	ポートVLAN利用時、タグVLANフレームは廃棄されます。
設定時の再起動の要否	ポートVLANの設定は即時反映されません。 機能を有効にするためには、装置の再起動が必要です。

[その他ルータ機能との連携に関する注意点]

VLANインタフェースでは、その他ルータ機能との連携に関して、以下の注意点があります。

○：制限なし　×：制限あり　△：一部制限あり　ー：対象外

機能	WA1020 WA1510 WA1511	WA2020 WA2021	備考
mdi/mdix設定	×	×	ポートVLANのSW-HUBポート単位で設定はできません。GE1.0で一括設定は可能です。（WA2020、WA2021）
speed/duplex設定	○	○	GE1.0でSW-HUBポート単位で設定が可能です。（WA2020、WA2021）
IPアドレス（固定IP設定）	○	○	IPv4のみ
IPアドレス（dhcp取得）	×	×	VLANインタフェースでは、dhcpクライアント設定はできません。
PPPoE	ー(WA1020) ×	×	VLANインタフェースでは、PPPoEインタフェースを割り当てることができません。
DHCPサーバ	○	○	
IPフィルタ	○	○	
MACフィルタ	×	×	VLANインタフェースでMACフィルタを利用できません。
tcp adjust-mss	○	○	
mtu設定	×	×	VLANインタフェースでは、MTU変更できません。ベースインタフェースのMTUサイズで動作します。
arp	○	○	
nat	×	×	VLANインタフェースでは、アドレス変換機能を利用できません。（ip nat enable）
napt	×	×	VLANインタフェースでは、アドレス変換機能を利用できません。（ip napt enable）
nat トラバーサル	×	×	
ルート設定	△	△	ip routeコマンドでの出力インタフェース設定において、dhcpオプションでVLANインタフェースを指定できません。
フローティングスタティック	○	○	
ip redirect	○	○	
VRRP	○	○	
IPSec	○	○	
ネットワークモニタ機能(event reach/unreach-host)	○	○	VLANインタフェースを出力インタフェースとしたICMP監視は可能です。
ネットワークモニタ機能（event interface）	×	×	監視するインタフェースにVLANインタフェースを指定できません。

機能	WA1020 WA1510 WA1511	WA2020 WA2021	備考
ネットワークモニタ機能(action)	×	×	link-up、up、down、link-downの指定が出来ません。
ブリッジ	×	×	VLANインタフェースはブリッジグループに参加できません。
EtherIP	×	×	VLANインタフェースで受信したEtherフレームをEtherIP機能にてカプセル化することはできません。
L2TPv3	×	×	VLANインタフェースで受信したEtherフレームをL2TPv3機能にてカプセル化することはできません。
proxy-dns	×	×	プロキシDNSサーバのアドレス登録として、VLANインタフェースを指定できません
dynamic dns	△	△	Dynamic DNSサービスのアカウント登録として､登録インタフェースに指定できません。
ping	○	○	
traceroute	○	○	
ftp	○	○	
tftp	○	○	
auto-verup	○	○	
netboot	×	×	VLANインタフェースからnetbootは出来ません。 また、boot entryコマンドによる登録インタフェースに指定できません。
show-tech	○	○	
IPアドレス通知機能	×	×	VLANインタフェースのUP/DOWNによるIPアドレス通知を行うことは出来ません。
syslog出力	○	○	VLAN機能に関するシスログの出力が可能です。
パケットダンプ	△	△	対象インタフェースにVLANインタフェースを指定できません。 また、VLANインタフェースを割り当てたベースインタフェースを指定すると､割り当てられたVLANインタフェースのパケットもダンプされます。
telnet	○	○	
Web-GUIへのログイン	○	○	
Web-GUIのVLAN関連設定	×	×	
NTP client	○	○	
SNMP	○	○	IF MIBのみ
privateMIB	×	×	
trap	○	○	

利用できるデータ通信端末

WAシリーズで使用できるデータ通信端末と適用できるインタフェースは以下となります。
（2014.7.01現在）

通信事業者	データ通信端末	適用インタフェース		Serial0 通信中のアンテナレベル取得※9	備考
		Serial0	Mobile Ethernet0.0		
NTT ドコモ	L-03D	○	○	×	LTE
	L-02C	○	○	×	LTE
	L-08C	○	×	×	HSPA
	L-07A	○	×	×	HSPA(PC カード) (※7)
	L-05A	○	×	×	HSPA (※1)
	L-02A	○	×	×	HSPA
	N2502	○	×	×	HSPA(PC カード)
	A2502	○	×	×	HSPA (※2)
イー・モバイル	GL03D	○	×	○	LTE
	GD01	○	×	×	HSPA
	D41HW	○	×	×	HSPA
	D33HW	○	×	×	HSPA
	D32HW	○	×	×	HSPA
	D31HW	○	×	×	HSPA
	D26HW	○	×	×	HSPA
	D23HW	○	×	×	HSPA
	D22HW	○	×	×	HSPA
	D21HW	○	×	×	HSPA
	D12HW	○	×	×	HSPA
	D21NE	○	×	×	HSPA(PC カード)
	D02NE	○	×	×	HSPA(PC カード)
IIJ モバイル	UX312NC	○	×	○	LTE
	510FU	○	○	○	LTE
	D31HW	○	×	×	HSPA (※3)
	D22HW	○	×	×	HSPA (※3)
	D02NE	○	×	×	HSPA(PC カード)
	120FU	○	×	×	HSPA (※3)
	110FU	○	×	×	HSPA (※3)
ソフトバンクモバイル	UX102NC	○	×	○	HSPA
	203HW	○	×	×	LTE
	004Z	○	×	×	HSPA
	C02HW	○	×	×	HSPA
	C02SW	○	×	×	HSPA

	C01SW	○	×	×	HSPA
	C02LC	○	×	×	HSPA
	C01LC	○	×	×	HSPA
au	USB STICK LTE HWD12	○	×	○	LTE(注 6) (モデムモード変換要)
	DATA07	○	×	×	CDMA
	DATA04	○	×	○	CDMA(PC カード) (※8)
	DATA03	○	×	○	CDMA/WiMAX (※5)
	DATA01	○	×	○	CDMA/WiMAX (※5)
	W07K	○	×	○	CDMA(PC カード) (※8)
	W06K	○	×	○	CDMA(PC カード) (※8)
日本通信	MF626	○	×	×	HSPA
	MF636	○	×	×	HSPA
NTT ｺﾐｭﾆｹｰｼｮﾝｽﾞ	UX302NC	○	×	○	LTE
	WM320	○	○	○	LTE
	MF121	○	×	×	HSPA
	MF120	○	×	×	HSPA
WILLCOM	HX008ZT	○	×	×	HSPA
	HX006ZT	○	×	×	HSPA
	HX003ZT	○	×	×	HSPA
	HX004IN	○	×	×	HSPA
	RX420IN (NS001U)	○	×	×	PHS (※4)

※1：PIN コード変更機能に対応していません。
※2：WA シリーズにて PIN コード関連の一部機能をサポートしておりません。
　　そのため、PIN コード操作を行わないようにしてください。
※3：事業者サービスとして、PIN 認証機能の利用が禁止されています。
　　WA シリーズにて PIN 認証に関する機能を利用しないでください。
※4：別途変換アダプタ NS001U が必要です。
※5：CDMA 通信のみ対応。WiMAX は使用不可です。
※6：WA シリーズでご利用いただくためには、KDDI 様提供の専用ツールによる、
　　HWD12 の動作モードの変更が必要です。
※7：別途変換アダプタ L01 が必要です。
※8：別途変換アダプタが必要です。
※9：サーベイモードは不要です。

ソフトウェア使用許諾契約書

重要－ご使用になられる前に、以下の使用許諾書を必ずお読みください。

本使用許諾契約書（以下「本契約書」といいます）は、下記に示されたソフトウェア（以下「本ソフトウェア」といいます）に関して、お客様（個人または法人のいずれかであるかを問いません）とＮＥＣプラットフォームズ株式会社（以下「ＮＥＣプラットフォームズ」といいます）との間に締結される法的な契約書です。

本ソフトウェアは、ＮＥＣプラットフォームズ製 UNIVERGE WAシリーズにインストールまたは同梱されており、お客様による本製品のご使用は、お客様が本契約書の条項に同意したものみなします。お客様が本契約書の条項に同意されない場合は、お客様は本ソフトウェアの使用をＮＥＣプラットフォームズから許諾されません。

本ソフトウェアの定義：本製品にインストールされたコンピュータプログラム一式、および同梱されるCD-ROMに含まれるソフトウェア、関連する印刷物（マニュアルなどの文書を含む）および電子ファイルをいいます。本契約では、本ソフトウェアには、ＮＥＣプラットフォームズまたはその販売元がお客様に提供した本ソフトウェアのアップグレード版、バグ修正版、改訂版（総称してアップグレード版）またはバックアップ・コピーが含まれます（これらには、この契約条件が適用されます）。

使用許諾：本契約書はお客様に以下の権利を許諾します。

(1) お客様は、本ソフトウェアを本製品においてのみ自己使用（社内使用）の目的だけに使用することができます。

(2) お客様は、バックアップ目的に限り、本ソフトウェアを任意の製品、媒体へ１部だけ複製することができます。

権利および制限

- **リバースエンジニアリング、逆コンパイル、逆アセンブルの禁止**：お客様は、本ソフトウェアをリバースエンジニアリング、逆コンパイル、または逆アセンブルすることはできません。
- **ソフトウェアの分離の禁止**：本ソフトウェアは１つの製品として許諾されます。その構成部分を分離して複数の本製品で使用することはできません。
- **レンタル**：お客様は、本ソフトウェアをレンタル、リースまたは貸与することはできません。
- **ソフトウェアの共用禁止**：お客様は、本ソフトウェアをリモートアクセスなどの方法により、複数のユーザと共用することはできません。
- **ソフトウェアの譲渡**：お客様は、お客様が購入された本製品とともに本ソフトウェアを恒久的に譲渡する場合のみ、本契約書に基づく権利を全て恒久的に譲渡することができます。ただし、譲受人が本契約書の条件に同意することを条件とし、当該譲渡以降、お客様は、一切の本ソフトウェア（バックアップ・コピーを含む）を保有することはできません。

解除：お客様が本契約書の条項および条件に違反した場合、ＮＥＣプラットフォームズは、他の権利を害することなく本契約を解除することができます。また、いかなる場合でも本契約が終了した場合、お客様は本ソフトウェアの使用を中止するとともに、本ソフトウェア、その複製物およびその構成部分を全て破棄しなければなりません。

保証：本契約に基づき、ＮＥＣプラットフォームズはお客様に対し本ソフトウェアに係る一切の保証を行いません。本製品の保証は、別途締結いただく保守契約の条件に従って行われます。

ＮＥＣプラットフォームズまたはその供給元は、いかなる法的構成をとるかに拘らず、本ソフトウェア、その使用もしくは使用不能から生じた、お客様の予測される収益もしくは利益、データの喪失、または特別損害、間接損害、結果的損害、偶発的損害もしくは懲罰的損害について、たとえＮＥＣプラットフォームズがかかる損害の可能性を知らされていたとしても、一切責任を負いません。ＮＥＣプラットフォームズまたはその販売元がお客様に対して負う契約上、不法行為（過失責任を含む）、またはその他の請求原因に基づく損害責任の範囲は、いかなる場合も、お客様が本製品の代金として支払われた価格を超えないものとします。

知的財産権：本ソフトウェアおよび本ソフトウェアの複製物についての著作権その他の知的財産権は、ＮＥＣプラットフォームズまたはその供給元が有しており、本契約により、本ソフトウェアのいかなる知的財産権もお客様に譲渡されるものではありません。

輸出：お客様は、日本政府および関連する外国政府の必要な許可を得ることなく、本ソフトウェアおよびその複製物を日本国から輸出してはなりません。

本契約書は日本国法に準拠するものとします。

第三者ソフトウェア：本ソフトウェアには The NetBSD Foundation, Inc.、WIDE Project、the OpenSSL Project、Eric Young氏、および the Regents of the University of California より許諾されたソフトウェアコンポーネントが含まれます。これらのソフトウェアコンポーネントには本契約の規定は適用されず、それぞれの使用許諾条件が適用されるものとします。これらのソフトウェア及びその使用条件の詳細は、コピーライトをご確認ください。